泉州师范学院数字校园使用手册

V2.00

泉州师范学院网络信息中心

二 00 九年九月

目录

前 言 4
第一章 泉州师范学院校园网简介 4
1.1 校园网概况 4
1.2 校园网络拓扑结构 5
1.3 泉州师范学院网络信息中心简介 5
1.4 网络信息中心工作职责 6
第二章 网络服务 6
2.1 校园网用户申请 IP 地址指南 6
2.2 校园网计费网关帐号开户指南 7
2.3 DNS 8
2.4 电子邮件 8
2.5 VPN 网络使用指南 9
第三章 信息服务 20
3.1 身份认证系统使用指南 20
3.2 信息门户使用指南 22
3.3 OA 系统使用指南 31
3.4 注册系统学生使用指南 32
3.5 内容管理系统使用指南 34
第四章 网络安全 36
4.1 上网安全基本策略 36
4.2 操作系统的常用安全设置 38
4.3 防病毒 41
4.4 防木马 42
4.5 防攻击 42
4.6 系统自动更新程序 Windows update 42
4.7 计算机的日常使用与维护 42
第五章 使用指南及常见问题解答 43
5.1 MAC 地址查询 43
5.2 IP 地址设置 44
5.3 锐捷客户端及安装说明 47
5.4 常见问题解答 47
第六章 政策法规 49
6.1 计算机信息网络国际联网安全保护管理办法 49
6.2 互联网电子公告服务管理规定 53
6.3 计算机病毒防治管理办法 56
6.4 中华人民共和国刑法(选摘) 59
第七章 校园网相关规定 60
7.1 泉州师范学院校园计算机网信息发布安全管理办法 60
7.2 泉州师范学院校园网二级管理规定 63
7.3 泉州师范学院校园网服务项目及收费标准 66
7.4 泉州师范学院校园网收费标准 71
7.5 泉州师范学院数字校园应用系统管理办法(试行) 74

第八章 资源和服务导航 79
8.1 校内网络与服务资源 79
8.2 网络服务导航和指南 79

前 言

泉州师范学院校园网已基本建成覆盖全校教学、科研、办公、图书馆、实验室以及学生公寓的快速校园网络，并逐步形成一个建设水平高、覆盖面积广、管理制度规范、资源和应用丰富、运行状况良好的校园网络环境。

随着校园网的投入使用，网络正以其高速、快捷、丰富的信息为学校的教学、科研、管理、服务提供越来越强大的支持。为方便广大用户使用校园网，了解我校网络运行方式及相关管理规定，并解答网络使用过程中出现的疑问，区分电脑自身故障与网络故障的不同而导致的网络不通等问题，提高网络使用效率和管理水平，做到有章可循、按章办事，我们特汇编了《泉州师范学院数字校园使用手册》。

本手册介绍了数字校园建设的总体情况、各种网络资源和应用系统的使用方法、网络基本知识、校园网管理规定以及校园网用户服务指南等内容，您可以通过使用这本手册来获得相关帮助，希望它能为您带来便捷和帮助。

随着政策的变化和管理技术上的不断升级，有些文件或文件中的部分规定会逐步修订，若有新文件颁布，均以最新文件规定为准。由于所编文件内容较多，涉及面较宽，手册中一定存在诸多不足之处，希望读者不吝赐教，以便我们修订、充实，逐步完善，充分发挥其在我校网络使用知识普及中的作用。

网络信息中心编委会

2009 年 9 月

(责任编辑:abanger)

第一章 泉州师范学院校园网简介

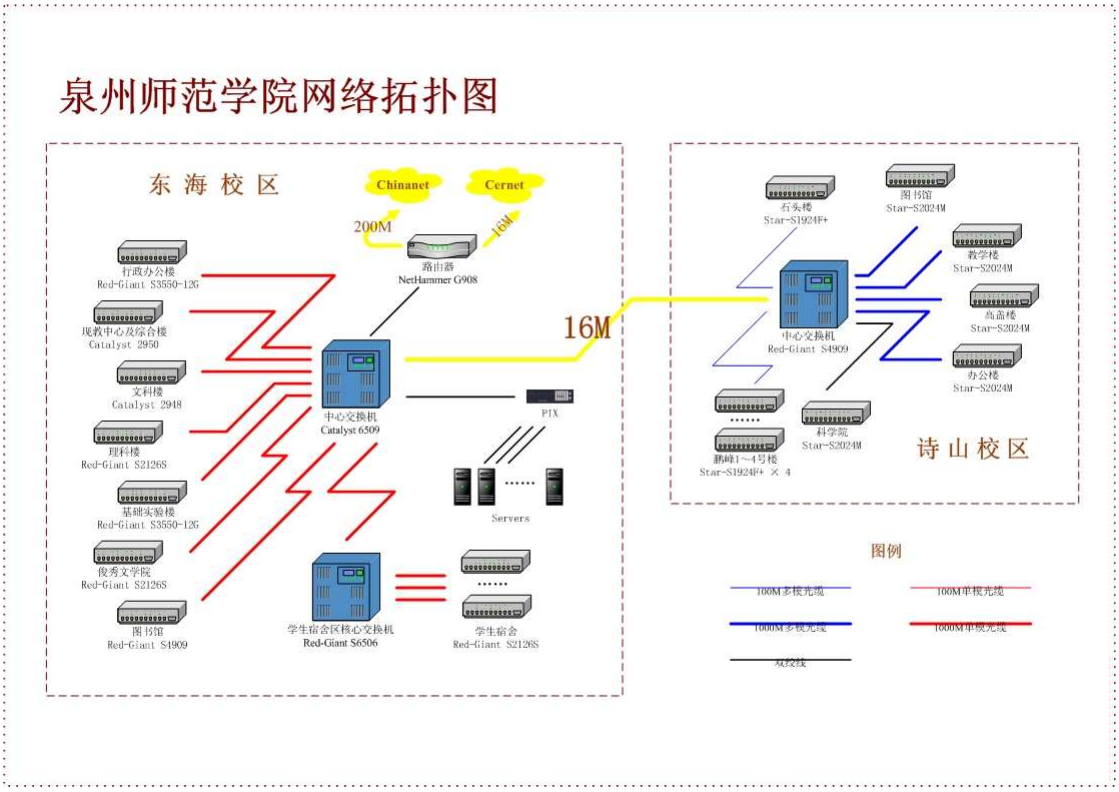
1.1 校园网概况

泉州师范学院校园网是中国教育和科研计算机网（CERNET）的节点。校园网经厦门大学接入 CERNET，经泉州电信连接中国电信网（CHINANET）。

校园网始建于 1998 年。现已建成的校园网主干为千兆，并可根据需求升级主干为万兆；主校区东海校区通过 16M 电路连接到诗山校区；各楼宇之间采用光缆连接，实现千兆主干，百兆到桌面的链路连接；目前 200M 连接到 CHINANET，16M 连接到 CERNET，总出口总带宽 216M。

校园网提供如下信息服务：电子邮件系统、FTP、瑞星网络版杀病毒软件系统、Windows 自动更新服务、VPN、“一卡通综合教务管理系统、网上教学支撑平台、科研系统、档案系统、人事管理系统、学工管理系统、信息发布系统等大量的网络应用系统。建立了一套在目录服务基础上的校园网用户身份认证和授权系统，初步实现了校园网用户的统一身份认证、统一门户、全校数据共享。

1.2 校园网络拓扑结构



1.3 泉州师范学院网络信息中心简介

网络中心建于 1998 年，设在崇福校区图书馆，鉴于我校计算机网络建设和信息化建设的整体考虑，于 1999 年正式改建为网络信息中心，随着学校主体搬迁东海校区， 2004 年 5 月中心主体搬迁到东海校区荣茂综合楼三楼。

现有专职技术人员 7 名，主要承担数字校园建设，包括校园网络和信息化的规划、建设、管理和维护。

网络信息中心的根本宗旨是为学校的教学、生活、科研和管理提供优良的信息与网络服务，创建高水平的数字校园环境。

1.4 网络信息中心工作职责

1、根据学校发展规划和信息化建设需求，组织起草学校信息化建设规划和实施方案；

2、参照国家有关标准，组织起草学校信息化建设相关标准和规范；

3、协助各职能部门进行需求分析，参与各应用系统开发，并承担系统运行和日常维护工作；

4、统筹协调学校校园网络的建设、改造及应用项目，监控网络运行情况，保证校园网络畅通；

5、负责制定学校信息化建设与管理的规章制度组织落实；

6、负责相关的技术指导与培训；

7、协助宣传部做好学校网站的建设、更新、维护；

8、协助宣传部、保卫处做好网络与信息安全工作。

9、学校领导交办的有关工作。

(责任编辑:abanger，图 chm)

第二章 网络服务

2.1 校园网用户申请 IP 地址指南

1、学生宿舍

在任意一台可以使用校园网的计算机上，进入 http://nic.qztc.edu.cn:8080/ip/ 页面，使用统一身份认证帐号登陆(还未获得统一身份认证账号的请携带本人身份证到中心领取账号密码)。登陆后根据 IP 申请系统提示如实填写个人信息以获

得自己的 IP 资源。

2、公共场所及办公场所

公共场所及办公场所的 IP 是以部门或者二级学院为单位进行分配的，由单位网络管理员申请 IP，也可由个人使用统一身份认证账号进行申请。申请得到 IP 后，参照<IP 地址设置>设置本机 IP；参照<MAC 地址查询办法>查询本机 MAC 地址后并用网线将网卡与网络端口连接。网卡指示灯亮起，计算机操作系统提示“本地连接电缆已连接”，保持电脑开机状态同时与网络信息中心联系（电话：22911950－0），网络信息中心工作人员及时予以开通。用户必须提供 MAC 地址用来开通网络端口。

3、家属区 IP

家属区 IP 是直接分配到每个住户，并公告在中心主页，请自行查询。

(责任编辑:cable)

2.2 校园网计费网关帐号开户指南

1、 教职工帐号申请

用户持本人有效证件或所在单位盖章证明(可由单位统一申请)，到中心办理。账号名即为本人工号。

2、 学生帐号申请

A 在校园网内任何一台可以上校内网的计算机上，进入 http://ipgate.qztc.edu.cn/页面，点击“用户注册”。

B 输入姓名及学号进行认证，在注册页面里依照备注说明认真填写注册信息。

C 注册成功后（不需要打印）执本人身份证或学生证至网络信息中心进行帐号激活。

D 请妥善保管好自己的帐号密码，所属帐号由本人负责。

3、注意事项

A 帐号密码遗忘、收费明细有疑问的，请执本人身份证至网络信息中心咨询。

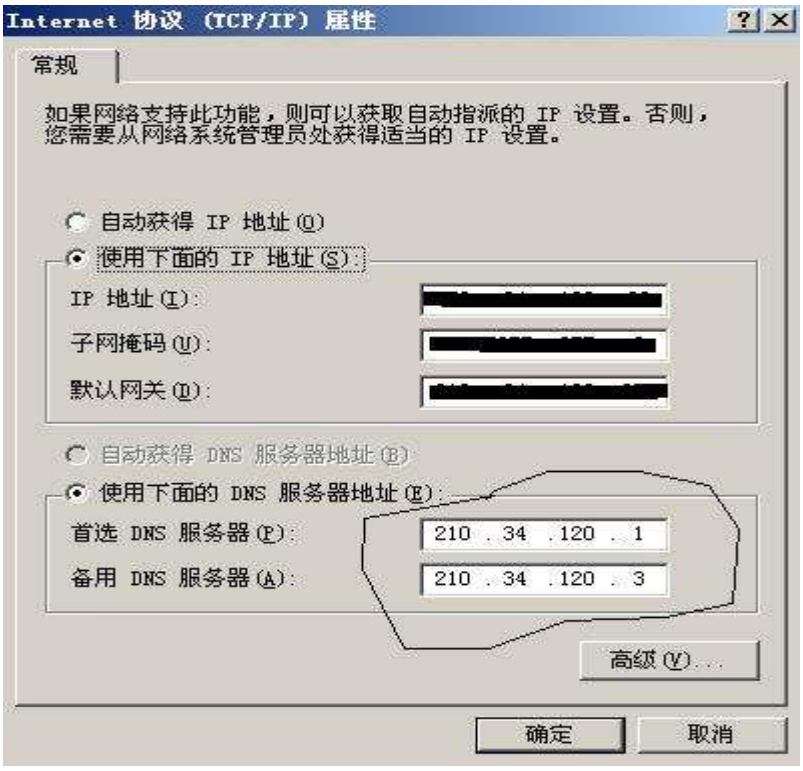
B 用户交费需购买充值卡充值。

(责任编辑:chm)

2.3 DNS

DNS，Domain Name System 或者 Domain Name Service（域名系统或者域名服务）。域名系统为 Internet 上的主机分配域名地址和 IP 地址。用户使用域名地址，该系统就会自动把域名地址转为 IP 地址。域名服务是运行域名系统的 Internet 工具。执行域名服务的服务器称之为 DNS 服务器，通过 DNS 服务器来应答域名服务的查询。

目前，我校的 DNS 服务器分别为：主域名服务器 210.34.120.1，备用域名服务器 210.34.120.3。请在 Internet 协议（TCP/IP）中配置如下图：



(责任编辑:chm)

2.4 电子邮件

2.4.1、在网络信息中心主页上下载《电子邮件申请表》，认真填写并单位盖章后，连同身份证复印件交到网络信息中心，由中心工作人员现场予以开通。

2.4.2、学校 EMAIL 服务器地址（web，pop3，web 服务）为：mail.qztc.edu.cn。

(责任编辑:chm)

2.5 VPN 网络使用指南

2.5.1 客户端操作

以 Windows 2000/XP 为例，其他操作系统略。

1、创建 VPN 连接

第一步：新建连接，**“开始”－>“设置”－>“网络和拨号连接”－>“新建连接”**；

如下图所示（单击创建一个新的连接，不同版本可能有所不一样）

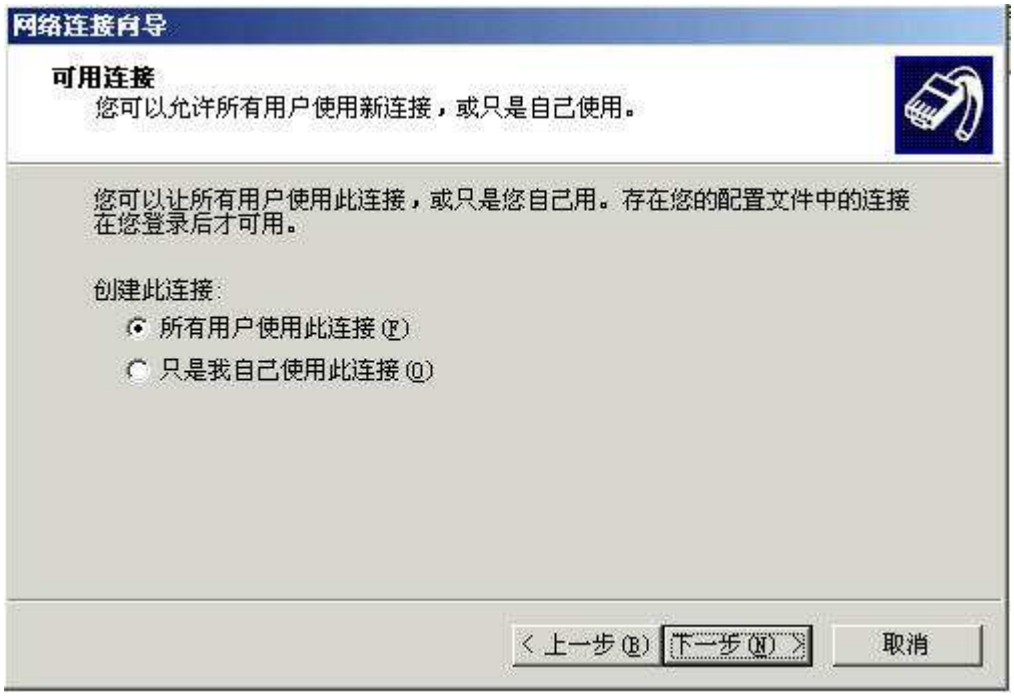
第二步：新建连接向导，单击“**下一步**”。

第三步：网络连接类型，选择“**通过 Internet 连接到专用网络**”

第四步：公用网络。选择“**不初始化连接（D）**”如果无这图出现，则跳过。

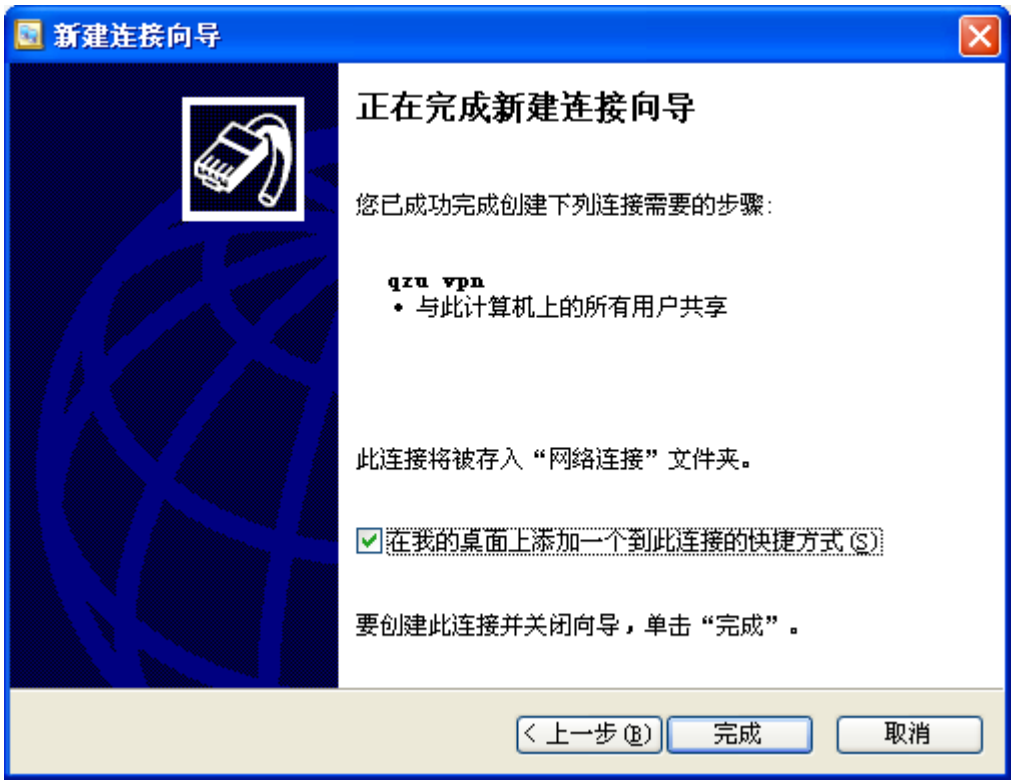
第五步：输入 VPN 服务器的地址：**59.61.216.61（接电信的用户），210.34.121.130（接广电的用户）**

第六步：选择可用连接，选择“**所有用户使用此连接（F）**”。



第七步：共享选择，确认“**启用此连接的 Internet 连接共享**”**没有打钩**。

第八步：在最后一步，你可以命名你所建的 VPN 连接的全称，如“QZU VPN”。为了方便使用，**建议选择在桌面上创建一个快捷方式**。



点击“完成”，你的 VPN 连接就创建完成了，下面就要在拨号对话框设置“属性”。

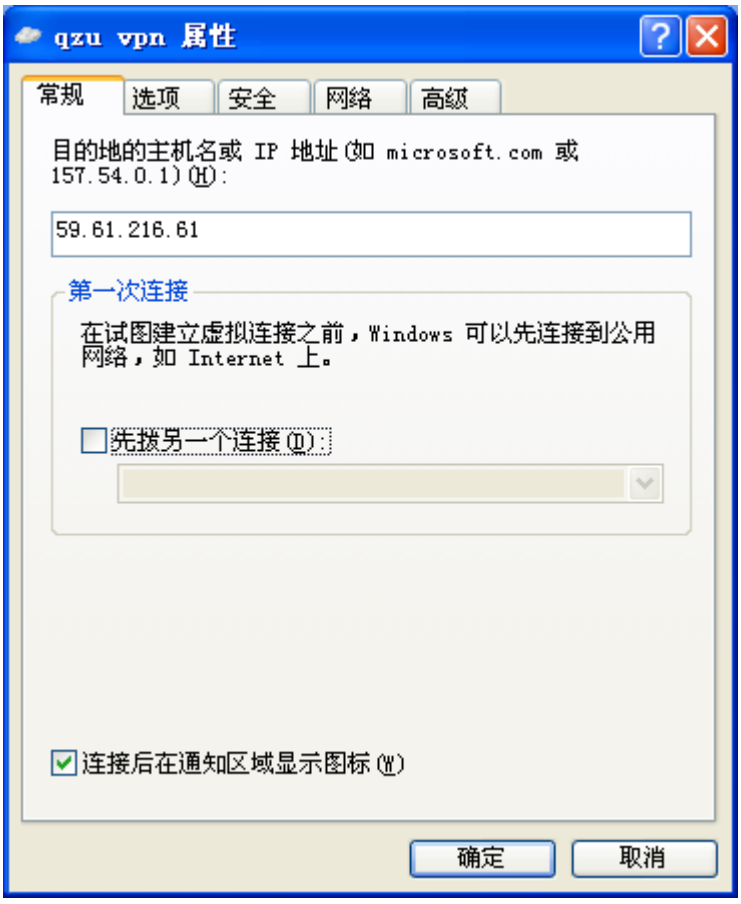
2、设置 VPN 属性

第一步：打开刚才新建的连接。点击桌面上的快捷方式，

，或从“开始”菜单里面选择。如下图：

第二步：在出现下面的对话框后，一般直接输入统一身份认证用户名和密码就能连接，还不能进行连接，需要对一些参数进行设置，单击“属性”，进入设置对话框。

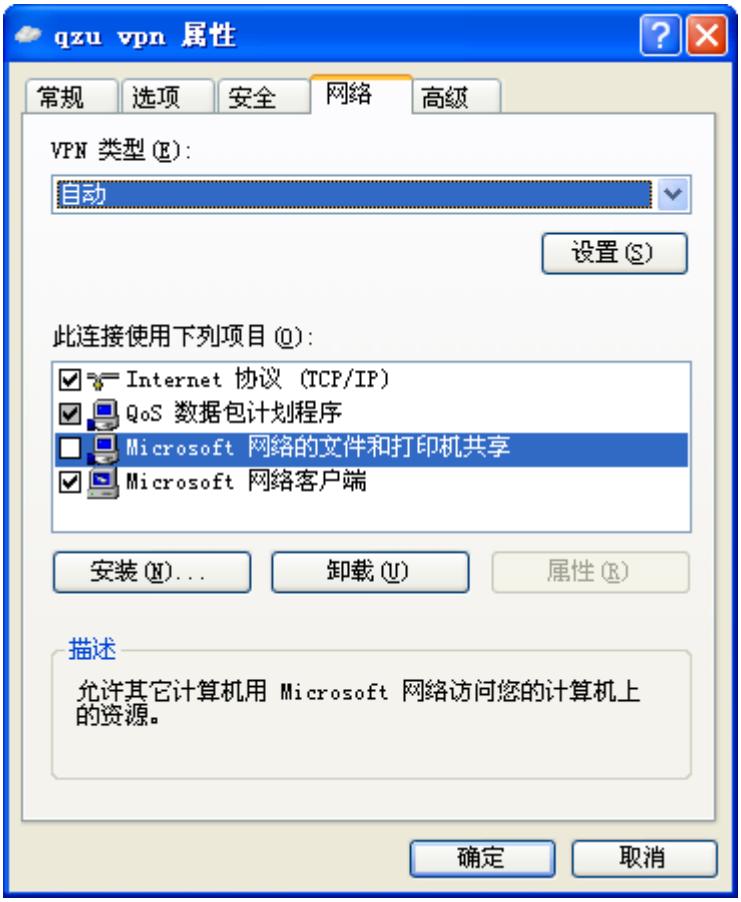
第三步：检查输入的 VPN 服务器的地址是否正确？



第四步：单击“安全措施”选项，默认情况下是“典型（推荐设置）”，在此，

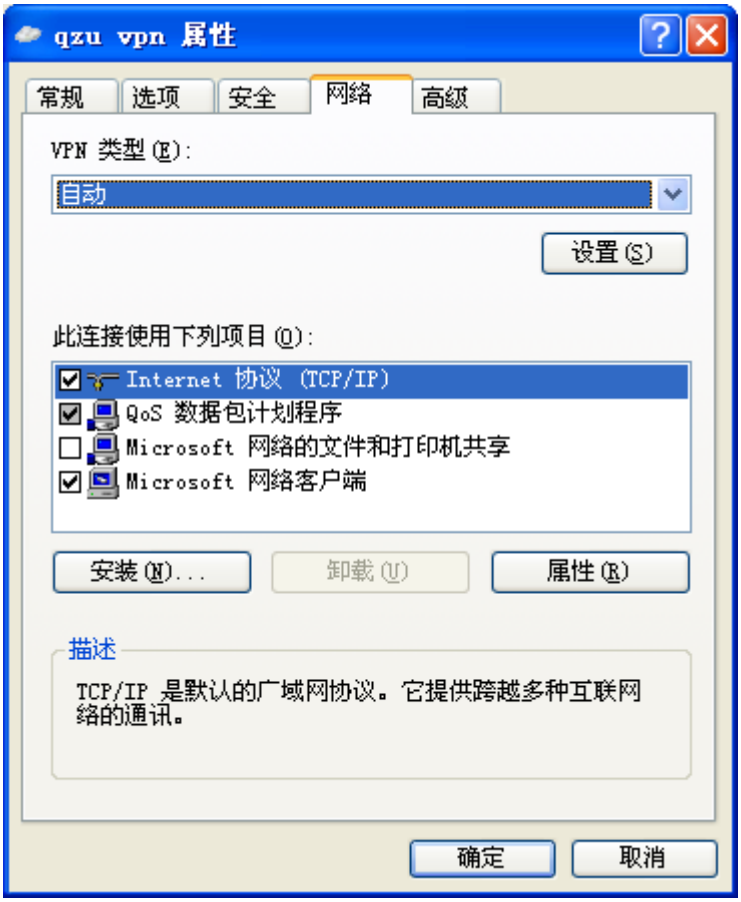
我们要选择下面的选项，即“**典型(推荐设置)**”。

第五步：单击“网络”选项,确定 Microsoft 网络的文件及打印机共享**没有打钩**,设置如下图



第六步：确认。选择“是”。

第七步：服务器类型。在“网络”选项，“VPN 服务器”类型选择“自动”



第八步：**配置结束，接下来就可以进行连接 VPN 服务器了：**

在连接对话框中输入您的 VPN 用户名和密码(即统一身份认证的账号密码)，点击“连接”。

连接成功后，在您的屏幕的右下角就会多出一个 VPN 网络连接的小图标，这表示已经连上泉州师院的校园网。

第九步：**上校园网：**现在您就可以像在校内一样使用校园网络资源了。

2.5.2 注意事项

1、 **如果个人电脑上有个人防火墙，**必须开放端口 1723 或关闭掉防火墙，停止保护功能，否则不能正常进行 VPN 拨号连接与访问。

2、 如不能正常进行认证，请确认 VPN 服务器地址是否为：**59.61.216.61（电信用户）或 210.34.121.130（广电用户）**

3、 如认证成功后，不能正常打开网页，请确认 VPN 拨号连接的 DNS 地址是否设置为：**210.34.120.1**

4、 如不能认证，请确认用户名与密码无误。

5、 在公共场合使用 VPN 服务时，请注意不要在“保存用户名和密码”的选项上打勾。

6、 使用在家带路由功能交换机可能无法正常连接，这问题暂时无法解决。

7、 在使用 vpn 拨号前不能上学校对外的服务器，否则至少 1 小时左右才能拨到 vpn 服务器。

8、 拨到学校 vpn 服务时，暂时无法使用其他网络。

9、 拨到学校 vpn 服务时，建议不要通过学校计费网关访问校外资源，尽管现在是开放的。

10、 由于电信或广电服务商分给我校的 IP 可能会有变化，请经常关注网络信息中心相关通知。

2.5.3 使用 VPN 常见问题

问：为什么要使用 VPN?

答：因为校内有很多 IP 地址在校外是无法访问的，学校图书馆购买的电子资源也只允许校内 IP 地址才可以访问，当您出差在外的时候，如果您希望访问校内资源或者使用学校图书馆购买的电子资源和学校内部通知等信息，您可以通过 VPN 访问这些资源。另外通过 VPN 访问校内资源可以保证您的机器和 VPN 服务器之间的传输是加密的，可以防止密码等一些敏感的信息被窃听。

问：使用 VPN 后就绝对安全了吗？

答：不，VPN 只能保证您的机器和 VPN 服务器之间传输的数据是加密传输的。但是，您通过 VPN 访问互联网的网站，在走出 VPN 服务器后的数据并不一定是加密传输的，所以不能保证那时候数据是否被窃听。

问：如何修改 VPN 的密码？

答：目前 VPN 是使用统一认证系统的，所以您只需修改您的统一身份认证的用户密码就可以正常工作了。

问：我是学生，请问我可以使用 VPN 吗？

答：不能，目前我们的 VPN 只是提供给校内教职工访问校内资源、图书馆电子资源，所以不提供给学生。

问：校内所有的应用 vpn 服务都提供吗？

答：不，我们只提供部分校内资源，将根据情况调整服务对象。

2.5.4 VPN 的申请

在网络信息中心主页上下载《VPN 服务承诺责任书》，认真填写并单位盖章后，交到网络信息中心，由中心工作人员现场予以开通。

(责任编辑:abanger)

第三章 信息服务

3.1 身份认证系统使用指南

身份认证系统是我校数字校园建设项目中的一个基础应用平台。由于校内存在多个应用系统，也因此产生了多个帐号和密码，不便于使用及管理。身份认证系统将全校教职员工、学生的信息和权限统一存放在一个公共的目录服务中，集中认证信息，最终目标是实现只使用一个帐号密码就能根据用户所属角色访问到校内所有的应用系统。

3.1.1 目前可使用或将使用统一身份认证的系统

1. 信息门户： http://my.qztc.edu.cn/
2. 教务系统： http://jwc.qztc.edu.cn
3. 注册系统： 登陆“信息门户后”即可在每学期初进行学籍注册
4. 学生管理系统： http://xg.qztc.edu.cn/epstar/login/index.jsp

5. 科研管理系统：http://nic.qztc.edu.cn:8080/keyan/

6. 人事信息管理系统：http://reg.qztc.edu.cn:9080/epstar/login/index.jsp

7. IP 地址申请： http://nic.qztc.edu.cn/ip

8. 宿舍上网： 采用 802.1x 认证的宿舍区使用的帐号密码

9. BBS： http://bbs.qztc.edu.cn/bbs/

10. 报修管理系统：http://apps2.qztc.edu.cn /mantis12/

11. OA 系统： http://oa.qztc.edu.cn/ （只对教职工开放）

12. VPN 服务： 填写 VPN 申请表至网络信息中心申请（只对教职工开放）

大部分业务都可通过信息门户访问到相应的应用系统，如学生通过信息门户可进行学籍注册等。其他校内应用系统（如电子邮件、计费网关、校选课、学生管理系统、一卡通查询等等）将随着数字校园建设的深入，不断集成到统一身份认证系统中。

3.1.2 统一身份认证的密码修改、找回

统一身份认证的初始密码为身份证号，用户可登陆信息门户后进行密码修改。首次登陆时需进行密码找回的设置，如遗忘密码则可通过密码找回功能重置密码。如果无法找回密码，则可携带本人有效证件至网络信息中心进行密码重置。

3.1.3 有关统一身份认证系统帐号使用注意事项

1. 全校所有用户的个人帐号有且仅有一个，教职工使用工号，学生使用学号。

2. 教职工的帐号和密码已通过 OA 系统（交办协交模块）发放到各单位秘书或办公室主任，请各单位注意查收并分发到教职工本人。

3. 学生的帐号为学号，初始密码为身份证号。

4. 所有用户在获得个人帐号信息后，请马上登陆到信息门户系统

http://my.qztc.edu.cn/修改密码！并牢记密码。

5. 密码丢失请带有效证件（身份证、学生证）到网络信息中心修改，不接受来电更改密码。

6. 请保护好自己的密码，不得转借他人使用，在公共场所使用之后，谨记**注销登陆**信息。帐号如被盗用请及时与网络信息中心联系并更改密码。

(责任编辑:chm)

3.2 信息门户使用指南

3.2.1 信息门户概述

在校园信息化建设中，存在包括教务、科研、人事、财务以及一卡通在内的多个业务系统，每个业务系统都会提供师生用户不同的信息服务，为提高师生用户的使用方便性和学校信息管理的一致性，需要在校内建立统一的信息服务门户平台，信息门户就是应此需求而产生的，通过信息门户平台，实现了以下几个功能，为我们带来很大的便利。

1. 整合网络资源功能：整合了校内网络资源的主页链接。

2. 个性化的主页设置与管理：提供满足用户个性化使用需求的界面自定义功能。任何人进入信息门户后台，即可对自己的门户进行管理，可以对几种不同的界面风格进行选择，可以添加新的栏目内容，对栏目进行命名，设置不同的排列组合，都可轻松实现。

3. 提供安全的登录手段，用于实现对各个子系统的单点登录，即：经由信息门户登录后，可通过点击相应子系统的链接，进入该应用系统中，而无需多次输入用户名、密码。

4. 提供了个人记事本、好友管理、个人收藏、个人文件夹、个人相册等大量的个人网上服务功能。

5. 提供全校和各部门的周历安排，以及周历查询功能。

6. 实现网上投票功能，该系统提供简单的在线调查，在线投票的设计、管理和投票结果的统计、显示。管理员可以动态的定制将要发起的投票项目，并可以将其配置给指定的用户。投票者可以在线填写选票，并提交。

7. 页面抓取功能，通过此功能可以集成不同应用系统的界面，比如集成教务处主页的通知以及外网的 Google 网站导航。

8. 集成了校内几个重要的应用系统，如人事系统、一卡通查询系统、学生管理系统、科研系统和财务系统等，进入信息门户后，学生和教职工都可对自己的一卡通消费情况进行查询；学生可以对自己每学期的成绩、助学信息、奖惩信息进行查询，教职工可以查询自己每个月的工资等，这些都为大家提供了很大的便利。

3.2.2 各功能模块的实例演示

1、整合了校内网络资源的主页链接

信息门户整合了校内大部分网络资源的主页链接，通过管理员的管理，随时可以对这些主页的链接进行添加、修改以及删除操作，可以进行栏目分类，自定义栏目名称。把所有校内网络资源的链接整合在一起，方便大家对各个主页的访问，省去记住很多个网址的麻烦。

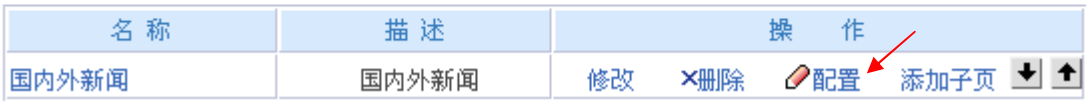
2、个性化的主页设置与管理

每个人用自己的账号、密码登录信息门户后，都可以对自己的门户界面进行配置。默认的主页已经有一些固定的配置栏目，但是每个人都可以根据自己的需要，设置自己的主页风格，能够添加、配置一些已有的信息资源。进入门户后，系统右上角如下所示：

首先，可以对整个门户的界面风格进行选择，点击上面的“改变风格”的链接，出现下面的界面：

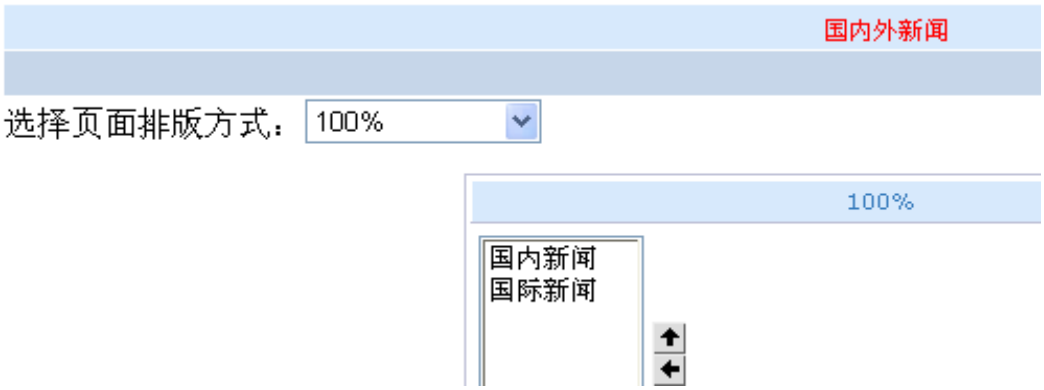
选定其中一种风格，点击上面的“保存”按钮，即可实现不同界面风格的转化。其次，点击上面的“页面管理”，出现如下界面：

在“添加页面”一栏下，自己命名一个“页面名称”，假设现在命名一个页面叫：国内外新闻，页面描述为：国内外新闻（对所要添加的页面进行比较详细描述），后点击“添加”按钮，出现如下界面：



点击右边的“配置”按钮，进入门户页面的配置，如下所示：

在“选择栏目”下，有许多不同分类的可选择配置，选中其中任何一个栏目，只需在它前面的方框中，打上勾，在上面的空白框就可以看到你选中的栏目，因现在我们想要配置一个有关国内外新闻的栏目，所以选中新闻信息下的“国内新闻”、“国际新闻”：



选择你所要添加的栏目后，还可以进行“选择页面排版方式”，点击下拉框，选择其中一种排版方式，比如：50%，50%。点击“↑ ← → ↓ ×”五个按钮进行移动和删除，此处先选中“国际新闻”，然后点击“→”，可以得到以下界面：

设置完毕后，点击右上角的“保存”按钮，点击“返回”按钮，即可退出自定义个性化设置，返回以下界面：

每个人根据不同的需要自定义自己的用户界面，可以不时地进行添加、修改以及删除操作，操作步骤重复上述过程即可。

3、单点登录功能

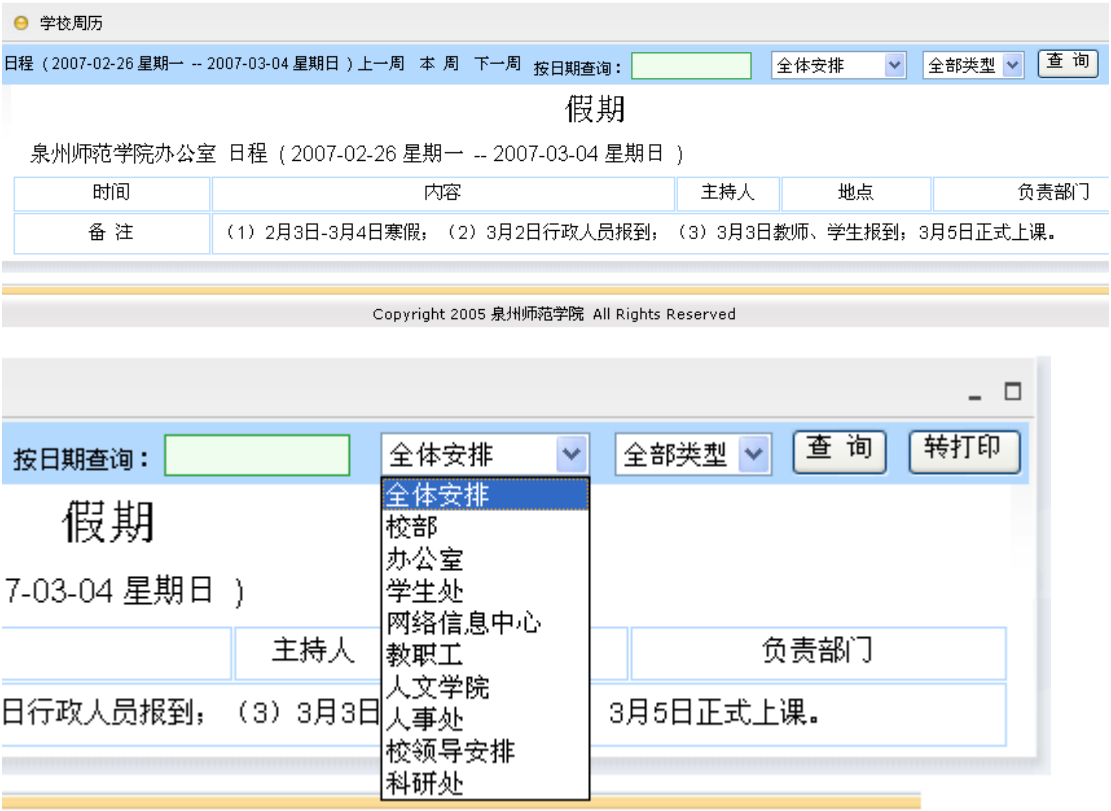
在下图的认证登陆配置中，输入相关系统的用户名和密码，点击“设置”，然后下次登录后，直接点击相应系统的链接，即可自动登

录，如点击“OA 集成”，即可进入你的 OA 系统。

4、个人网络服务功能

信息门户提供了个人记事本、好友管理、个人收藏、个人文件夹、个人相册等个人网上服务功能。

5、提供全校和各部门的周历安排，以及周历查询功能



6、实现网上投票功能

（暂时省略）

7、页面抓取功能

信息门户实现了页面抓取功能，通过管理员的配置，可以集成不同应用系统的界面，比如现在集成了教务处主页的通知，也可以集成外网的应用界面。

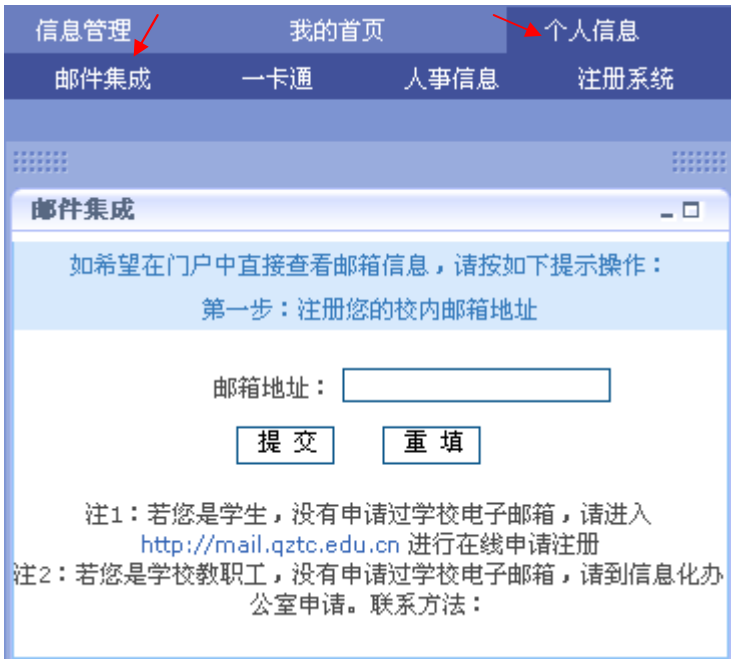
邮件集成
一卡通
人事信息
注册系统
个人自助
实用网站链接
hao123实用酷站精选
文 学 起点 榕树下 小说阅读网 潇湘书院 红袖添香 幻剑书盟 更多>>
游 戏 17173 新浪游戏 太平洋游戏 小游戏 中国游戏中心 游戏中国 更多>>
下 载 天空软件 华军软件 霏凡软件站 ZOL下载 新浪下载 太平洋下载 更多>>
军 事 中华网军事 新浪军事 新华网军事 铁血军事 千龙军事 更多>>
音 乐 QQ163音乐网 MP3下载 要听音乐 天籁之音 yymp3 百度MP3 更多>>
邮 箱 新浪邮箱 TOM邮箱 雅虎邮箱 163邮箱 126邮箱 搜狐邮箱 Hotmail 更多>>

8、集成了校内几个重要的应用系统

信息门户集成了校内几个重要的应用系统，如人事系统、注册系统、一卡通查询系统、学生管理系统、电子邮件系统等。进入信息门户后，学生和教职工都可对自己的一卡通消费情况进行查询;学生可以对自己每学期的成绩、助学信息、奖惩信息等进行查询，教职工可以查询自己每个月的工资，有学校电子邮件的人

员，通过设置，每次都可以点击直接进入电子邮件，无需输入账号、密码，这些都为大家提供了很大的便利。

信息门户集成了校内电子邮件，第一次进入邮件集成时，可以看到以下画面，请设置你的**校内电子邮件**，然后登录到邮箱中收取注册密码，填入验证码后，进入邮箱。以后每次点击“进入邮箱”的链接，即可进行快速登录校内电子邮件，如果邮箱密码或者更换邮箱账号时，点击：重新设置邮箱信息，重新进行设置。



当然，信息门户还有一些功能没有介绍完整，本手册介绍的是其中主要的一些功能，其余的功能有待用户深入接触后，慢慢体验，阅读文档完，使用过程如还发现有什么问题，可以致电网络信息中心。

(V070322,责任编辑:zqc)

3.3 OA 系统使用指南

暂 略

(责任编辑:xulu)

3.4 注册系统学生使用指南

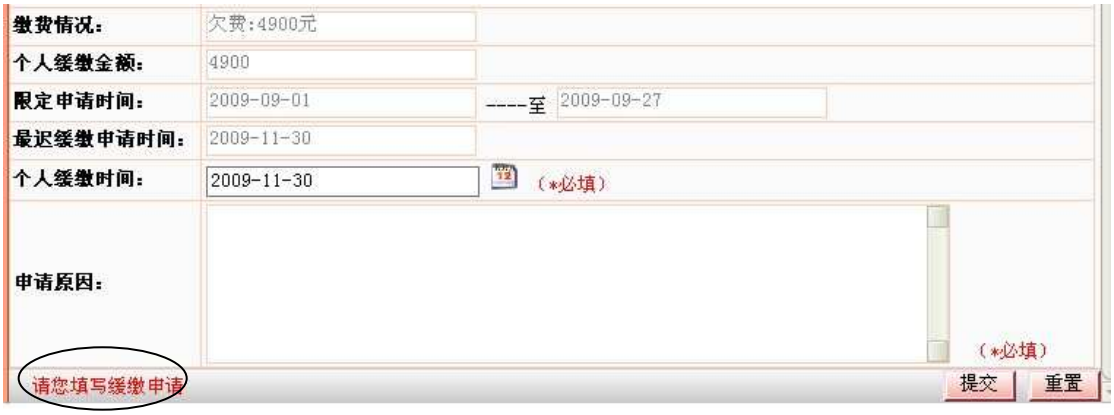
登陆信息门户平台 http://my.qztc.edu.cn,出现界面，在登录框中输入用户名和密码：

进入系统后，将会出现你的缴费情况和注册情况界面：

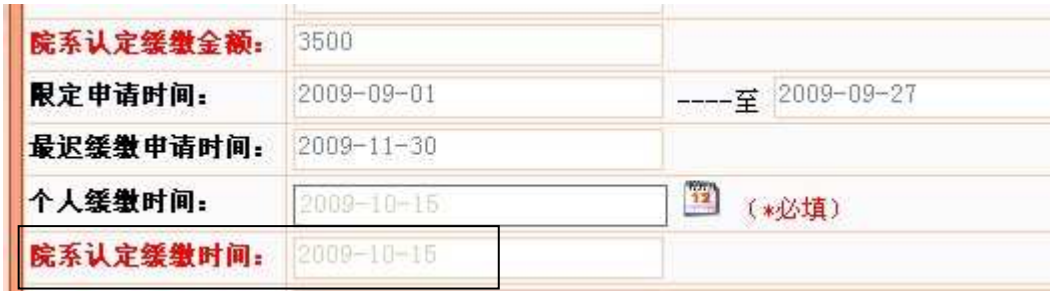
1、 如果你已经正常缴费，页面下面的“注册”按钮显示为黑色，你直接点击下面的“注册”按钮即可完成注册，注册成功后，页面的左下角会出现已经注册成功的提示，此时“注册”按钮为灰色，不能再进行注册了。

2、如果你还没有正常缴费，此时“注册”按钮是灰色的，无法注册，你只能进行学费缓缴申请，想要办理贷款的同学，也是先进行缓缴申请，点击页面左边的“学费缓缴申请”链接：

修改“个人缓缴时间”，把“申请原因”框的信息按照要求填写一下，点击“提交”，等待学院教务科的老师审批通过后，左下角会有“审批通过”的提示，即可按照第一步的步骤，进行正常注册了。



注：申请缓缴审批通过后，如果依然无法注册，请到缓缴的页面中查看一下“院系认定缓缴时间”，如果你已经超过院系认定的缓缴时间的话，也会无法注册，此时，你可以到学院的教务科请教务科的老师帮你修改一下“院系认定缓缴时间”，把时间延后一些，就能正常注册了。



(责任编辑:zqc)

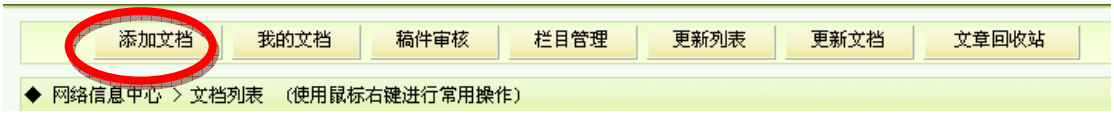
3.5 内容管理系统使用指南

1、输入网址：http://cms.qzu.cn/decms/index.html，在首页面的下方，点击页下角“友情链接”的“CMS 后台管理”：

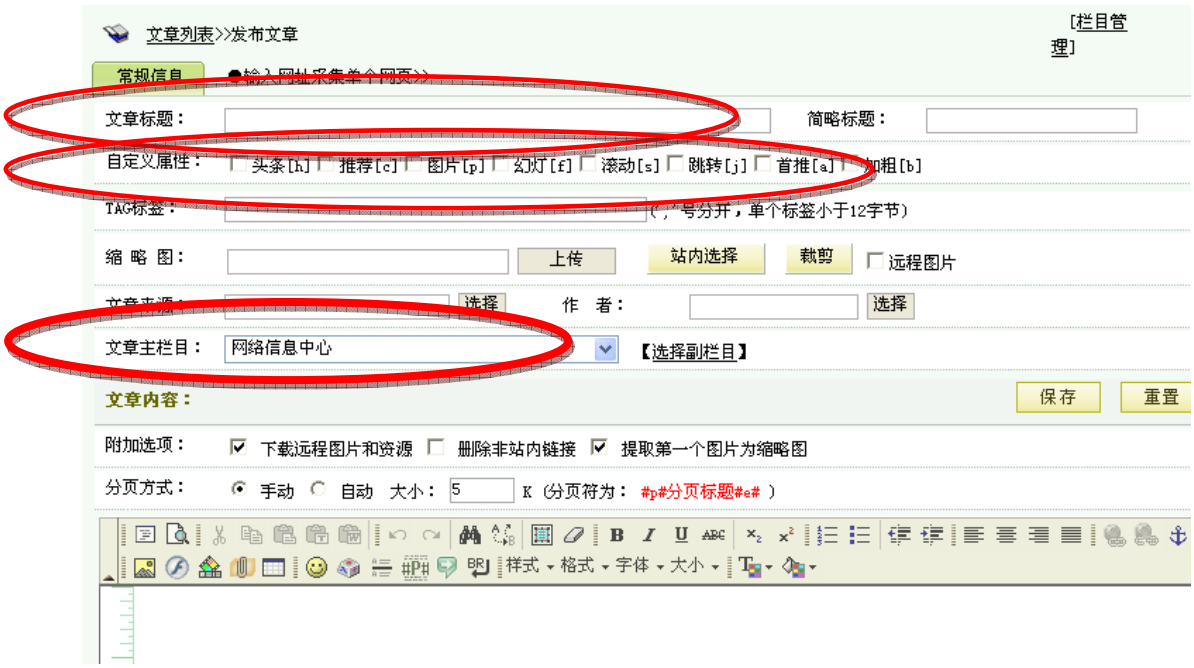
2、页面会跳转到后台管理网页，输入用户名和密码：

3、进入系统后点“等审核的档案”或“我发布的文档”

4、右边出现：



5、发布信息点“添加文档”



发布信息主要填写：

“文章标题”

“自定义属性”几个属性特点：

“校内通知”：发布的信息将放在信息最前面，并在信息门户的通知栏目上显示

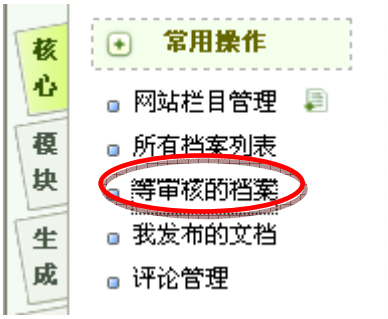
“推荐”：发布的信息将出现在网站主页“推荐内容”

“图片”：发布的信息将出现在网站主页“图文资讯”

“校外公告”：发布的信息将在学校主页的公告栏上显示

“文章主栏目”——选择要发布信息所属栏目

6、信息保存后点“等审核的档案”



选择要审核的文章，然后点“审核”

◆ 学生处 > 文档列表 （使用鼠标右键进行常用操作）
ID 选择 文章标题 录入时间 类目 点击 HTML 权限 发布人 操作
14210 e 2009-04-17 学生处 0 未生成 待审核稿件 test 编辑 | 预览
14209 E 2009-04-17 奖惩工作 1 未生成 待审核稿件 test 编辑 | 预览
全选 取消 更新 审核 推荐 移动 删除

7、到此信息发布成功，可点“网站主页” 查看

第四章 网络安全

网络已成为病毒传播的第一途径，疏于安全防范的联网计算机不仅会使自己的数据、文件于危险的境地，还可能成为各类蠕虫病毒，木马程序的温床和跳板，被利用向网络中的其他计算机发起扫描和攻击。这不但会严重干扰校园网络的正常运行，还同时给我校校园网的形象带来了负面影响。为有效遏止校园网安全的各种不利因素，提高用户安全防范意识，在本章向用户介绍一些安全防护常识，希望大家遵守相关的计算机网络信息安全法律法规，共同防范未然，树立“网络安全从我做起”的观念，共同创造安全的校园网环境。

4.1 上网安全基本策略

1 树立网络安全意识，加强自我防范意识。

2 在进行任何的交易或发送信息之前阅读网站的隐私保护政策。因为有些网站会将你的个人信息出售给第三方。

3 网上购物时，确定你采用的是安全的连接方式。你可以通过查看浏览器窗口角上的闭锁图标是否关闭来确定一个连接是否安全。

4 在线时不要向任何人透露个人信息和密码。黑客有时会假装成 ISP 服务代表并询问你的密码。请谨记：真正的 ISP 服务代表是不会问你的密码的。

5 使用较复杂的密码，防止他人盗用，减少受恶意攻击的几率，经常更改你的密码，使用包含字母和数字、位数不小于 8 位的密码，从而干扰黑客利用软件

程序来搜寻最常用的密码。

6 在不需要文件和打印共享时，关闭这些功能。文件和打印共享有时是非常有用的功能，但是这个特性也会将你的计算机暴露给寻找安全漏洞的黑客。一旦进入你的计算机，黑客就能够窃取你的个人信息。

7 不要打开来自陌生人的电子邮件附件。不要随意运行邮件内的附件（比如“ .exe ”文件，“ .chm ”文件等等。），这些附件可能包含一个特洛伊木马程序，该程序使得黑客能够访问你的文档，甚至控制你的外设。

8 及时更新最新的操作系统补丁程序.

9 安装一个防病毒程序保护你免受病毒、特洛伊木马程序和蠕虫侵害。及时安装、更新升级杀毒软件并启动杀毒软件的实时监控功能，应定时启动杀毒软件对硬盘进行查杀病毒的处理。

10 安装一些的木马专杀工具。可以确定你的计算机是否具备防护病毒和恶意代码的能力，扫描你的计算机查找安全漏洞和病毒。

11 安装个人防火墙。使用个人防火墙防病毒程序以防黑客攻击和检查黑客程序。个人防火墙能够保护你的计算机和个人数据免受黑客入侵，防止应用程序自动连接到网站并向网站发送信息。

12 不要随意打开一些网站弹出的广告窗口。

13 谨慎使用可移动存储介质，如 U 盘的使用，在拷贝文件时应检测有无病毒存在后使用，避免病毒通过 U 盘在电脑间传播。打开 U 盘时养成良好的习惯，不要双击盘符打开 U 盘，而应该右键单击盘符再选择打开或者资源管理器，这样可以有效避免 autorun 病毒的感染。

14 对公共、共享软件或各种资料的使用要小心谨慎，不要从一些非正规网站下载安装不明软件和资料；

15 各部门在学院网站上发布信息时应将要上传的文件查杀病毒，确保文件无病毒后再上传发布信息。

16 及时清空浏览器的缓存和历史纪录。

17 最重要一点：经常备份您的重要文件，减少病毒灾难或电脑故障而受到的损失。

4.2 操作系统的常用安全设置

主要针对使用 Windows 操作系统，其他操作系统暂略。

1 无论是从光盘安装操作系统，还是从硬盘安装，都请使用比较新的已经集成部分 ServicePack 的版本(Windows2000 内置 SP4，WindowsXP 内置 SP2)。

2 操作系统安装应遵循最小化安装原则，凡是不需要使用的系统组件、协议、和系统服务，特别是网络服务都不要安装。

3 安装操作系统之前一定要先拔下网线，在离线状态下进行安装。

4 建议至少分三个磁盘分区。第一个分区用来安装操作系统，第二分区存放重要的数据和日志文件，第三个分区作为备份。建议安装计算机中的所有分区都尽可能去使用 NTFS 格式，NTFS 分区能够提供 FAT、FAT32 或 FAT32x 文件系统所不能提供的访问控制与保护。

5 安装过程中或结束后必须要设置可靠的用户口令，建议把 Administrator 这个系统默认的超级用户重命名为不明显的名字(例如，不具有“admin”或“root”等标记)，并给一个足够复杂的口令（不少于 9 个字符，并包括特殊字符)，禁用所有非活动帐户，删除不再需要的帐户，如果来宾帐户（Guest）已启用，请将其禁用。

6 操作系统安装完成后，应立即安装系统最新的 Service Pack，然后才能联网，否则几分种以内，就可能被蠕虫病毒利用系统漏洞感染。(可以先从 http://wsus.qzu.cn/ 事先下载有关重要系统补丁并复制到您的计算机上)。

7 关闭不必要的有安全隐患的服务

用户可以根据实际情况，关闭表 1 中所示的系统自动运行的有安全隐患的服务。

我们建议您对服务作如下配置（“默认”为系统初始设置，“基准”是我们建议的设置)。

表 1

Windows 服务配置参考			
服务	**全称**	**默认**	**基准**
Alerter	Alerter（警报器）	自动	禁用
AppMgmt	Application Management（应用程序管理）	手动	禁用

ClipSrv	ClipBook（剪贴簿）	手动	禁用
EventSystem	COM+ Event System（COM+ 事件系统）	手动	手动
Browser	Computer Browser（计算机浏览器）	自动	禁用
DHCP	DHCP Client（DHCP 客户）	自动	自动
Dfs	Distributed File System（分布式文件系统）	自动	仅在 域控制器 角色中启用
TrkWks	Distributed Link Tracking Client（分布式链接跟踪客户）	自动	自动
TrkSrv	Distributed Link Tracking Server（分布式链接跟踪服务器）	手动	禁用
MSDTC	Distributed Transaction Coordinator（分布式事务协调器）	自动	禁用
DNSCache	DNS Client（DNS 客户）	自动	自动
EventLog	Event Log（事件日志）	自动	自动
Fax	Fax Service（传真服务）	手动	禁用
NtFrs	File Replication（文件复制）	手动	禁用
IISADMIN	IIS Admin Service（IIS 管理服务）	自动	禁用
Cisvc	Indexing Service（索引服务）	手动	禁用
SharedAccess	Internet Connection Sharing（Internet 连接共享）	手动	禁用
IsmServ	Intersite Messaging（站间消息传递）	禁用	禁用
PolicyAgent	IPSEC Policy Agent(IPSEC Service)（IPSEC 策略代理程序（IPSEC 服务））	自动	禁用
Kdc	Kerberos Key Distribution Center（Kerberos 密钥分发中心）	禁用	仅在 DC 角色中启用
LicenseService	License Logging Service（许可证记录服务）	自动	禁用
Dmserver	Logical Disk Manager（逻辑磁盘管理器）	自动	自动
Dmadmin	Logical Disk Manager Administrative Service（逻辑磁盘管理器管理服务）	手动	手动
Messenger	Messenger（信使）	自动	禁用
Netlogon	Net Logon（网络登录）	自动	自动
Mnmsrvc	NetMeeting Remote Desktop Sharing（NetMeeting 远程桌面共享）	手动	禁用
Netman	Network Connections（网络连接）	手动	手动
NetDDE	Network DDE（网络 DDE）	手动	禁用
NetDDEdsdm	Network DDE DSDM（网络 Network DDE DSDM）	手动	禁用
NtLmSsp	NTLM Security Support Provider（NTLM 安全支持提供程序）	手动	禁用
SysmonLog	Performance Logs and Alerts（性能日志和警报）	手动	手动
PlugPLay	Plug and Play（即插即用）	自动	自动
Spooler	Print Spooler（打印后台处理程序）	自动	仅在"文件和打印"角

			色中启用
ProtectedStorage	Protected Storage（受保护存储）	自动	自动
RSVP	QoS Admission Control (RSVP)（QoS 许可控制 (RSVP)）	手动	禁用
RasAuto	Remote Access Auto Connection Manager（远程访问自动连接管理器）	手动	禁用
RasMan	Remote Access Connection Manager（远程访问连接管理器）	手动	禁用
RpcSs	Remote Procedure Call（远程过程调用，RPC）	自动	自动
Rpclocator	Remote Procedure Call (RPC) Locator（远程过程调用 (RPC) 定位器	手动	仅在 DC 角色中启用
RemoteRegistry	Remote Registry Service（远程注册表服务）	自动	禁用
NtmsSvc	Removable Storage（可移动存储）	自动	禁用
RemoteAccess	Routing and Remote Access（路由和远程访问）	禁用	禁用
Seclogon	RunAs Service（RunAs 服务）	自动	禁用
SamSs	Security Accounts Manager（安全帐户管理器）	自动	自动
Lanmanserver	Server（服务器）	自动	自动
SMTPSVC	Simple Mail Transport Protocol（简单邮件传输协议，SMTP）	自动	禁用
ScardSvr	Smart Card（智能卡）	手动	禁用
ScardDrv	Smart Card Helper（智能卡助手）	手动	禁用
SENS	System Event Notification（系统事件通知）	自动	自动
Schedule	Task Scheduler（任务计划程序）	自动	禁用
LmHosts	TCP/IP NetBIOS Helper Service（TCP/IP NetBIOS 支持服务）	自动	自动
TapiSrv	Telephony（电话服务）	手动	禁用
TlntSvr	Telnet（远程登录协议）	手动	禁用
TermService	Terminal Services（终端服务）	禁用	禁用
UPS	Uninterruptible Power Supply（不间断电源）	手动	禁用
UtilMan	Utility Manager（工具管理器）	手动	禁用
MSIServer	Windows Installer（Windows 安装服务）	手动	禁用
WinMgmt	Windows Management Instrumentation（Windows 管理规范）	手动	禁用
WMI	Windows Management Instrumentation Driver Extensions（Windows 管理规范驱动程序扩展）	手动	手动
W32Time	Windows Time（Windows 时间服务）	自动	自动
Workstation	WorkStation（工作站）	自动	自动
W3svc	World Wide Web Publishing Service（万维网发布服务）	自动	仅在 IIS 角色中启

			用

8 关闭系统默认共享

方法一：采用批处理文件在系统启动后自动删除共享。 首选在 Cmd 提示符下输入“Net Share”命令，查看系统自动运行的所有共享目录。然后建立一个批处理文件 SHAREDEL.BAT，将该批处理文件放入计划任务中，设为每次开机时运行。文件内容如下：

```
NET SHARE C$ /DELETE
NET SHARE D$ /DELETE
NET SHARE E$ /DELETE
……
NET SHARE IPC$ /DELETE
NET SHARE ADMIN$ /DELETE
```

方法二：修改系统注册表，禁止默认共享功能。在 Local_Machine\System\CurrentControlSet\Services\Lanmanserver\parameters 下新建一个双字节项“auto shareserver”，其值为“0”。

9 删除多余的不需要的网络协议

删除网络协议中的 NWLink NetBIOS 协议，NWLink IPX/SPX/NetBIOS 协议，NeBEUI PROtocol 协议和服务等，只保留 TCP/IP 网络通讯协议。

4.3 防病毒

计算机病毒通过网络传播速度惊人，危害大，又常常难以根除。建议用户在各自的电脑上安装杀毒软件。要升级杀毒软件才能有效抵御新病毒的偷袭，建议使用学校正版的网络版瑞星杀病毒软件，软件下载地址：ftp://210.34.120.2/Software/安全相关/瑞星网络版杀毒软件(校内使用)/，瑞星杀病服务器网关 210.34.120.3。升级后要全面清查一次。若用户自行安装其它品牌的杀毒软件，请尽量购买、安装正版的软件，并经常升级病毒库，以对付最新出现的病毒。

4.4 防木马

大量木马、流氓软件、间谍软件都可能会导致系统运行异常,而这类软件往往不会被防病毒软件所识别处理，您可以专门工具补丁来获取清除软件，可到 ftp://ftp.qztc.edu.cn/Software/安全相关/ 找到部分工具。推荐使用 360 安全卫士或者瑞星卡卡上网安全助手。

4.5 防攻击

安装防火墙是防攻击的一个好方法。使用操作系统自带的防火墙或个人防火墙防病毒程序以防黑客攻击和检查黑客程序;能够保护你的计算机和个人数据免受黑客入侵，防止应用程序自动连接到网站并向网站发送信息。

4.6 系统自动更新程序 Windows update

我们使用的 windows 操作系统已经历了好多版本，各个版本中都有着各种各样的安全漏洞。一些安全漏洞，可轻易掌控您的计算机、能够为部分病毒所利用、轻易感染和破坏您的计算机。

请及时为系统或其他应用软件打补丁。学校设有 Windows 系列操作系统补丁服务器：http://wsus.qzu.cn/，使用说明就在此网站上。使用此更新同微软的在线升级并无冲突，您仍然可以随时访问 http://windowsupdate.microsoft.com 来进行在线升级。一定要及时为操作系统系统打上补丁，否则一些病毒就无法清除干净。不厌其烦地安装补丁程序，任何一种软件都在不停地进行升级，这主要是因为软件都有不完善之处，包括存在一些安全漏洞。

4.7 计算机的日常使用与维护

1 定期关注我们在 http://my.qztc.edu.cn 校内网络安全网站发布的安全公告和安全建议。

2 定期做好重要个人文件的数据备份工作，取消所有不必要的文件共享,以

防止可能的数据泄漏，所有必要的文件共享要设置适当的共享级别访问权。

3 上网时，若经常出现电脑蓝屏、莫名其妙地死机、电脑受到控制等，则要断开网络连接，采取措施清除黑客程序，必要时重新格式化硬盘，重装操作系统，以绝后患。

(责任编辑:abanger)

第五章 使用指南及常见问题解答

5.1 MAC 地址查询

5.1.1 使用 Windows XP、VISTA 或 Windows 2000 的用户

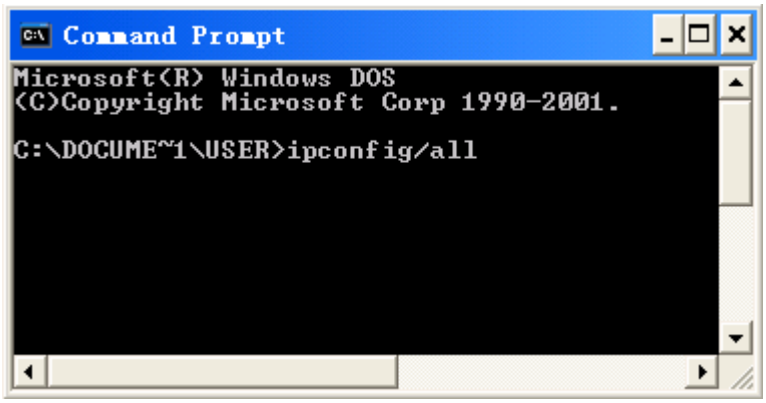
1、打开“开始”菜单。用鼠标左键单击屏幕左下角的“开始”。

2、用鼠标左键单击“运行”项。

3、在出现的工作窗口中填入：command 或者 cmd 。如图。

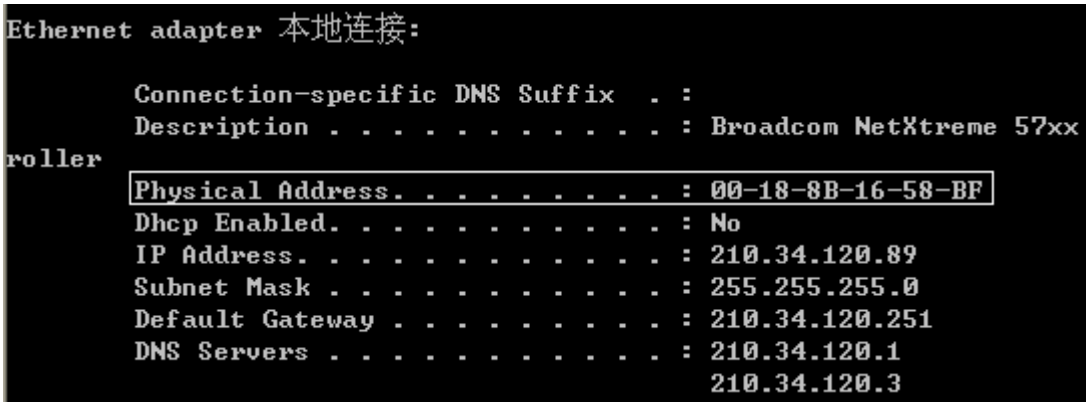
后点击“确定”。

4、出现如下图所示画面。



如图中所示，输入命令：ipconfig/all 或者 ipconfig –all ，回车。

5、下图中方框框出的内容就是 MAC 地址。



5.2 IP 地址设置

5.2.1 vista 系统中 设置 IP 地址

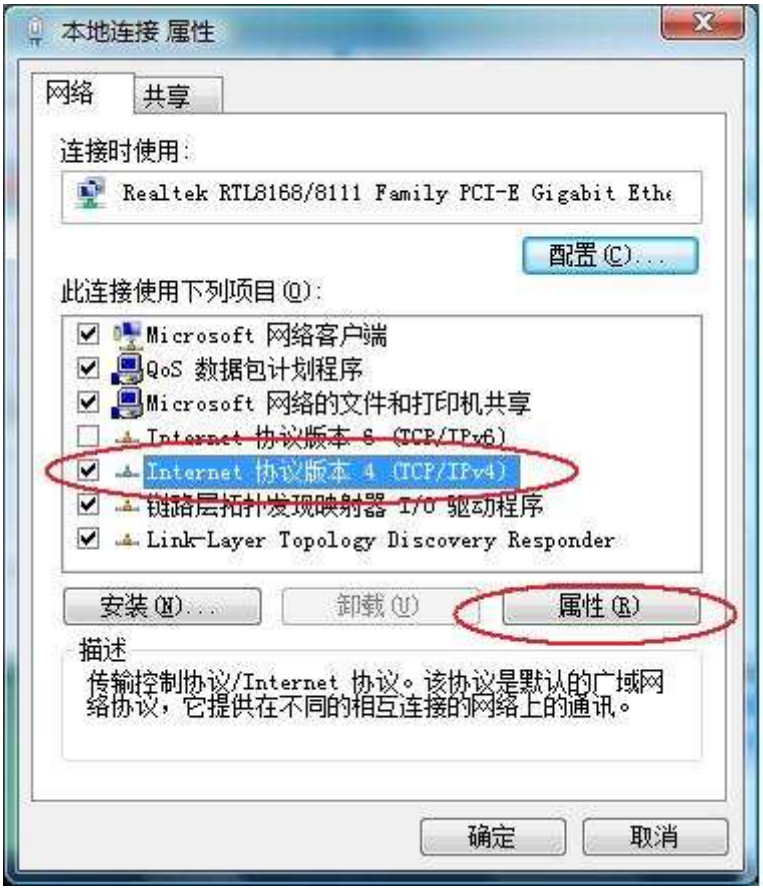
Vista 系统中 IP 地址的设置方法

第一步：右击桌面“网络”图标，点击“属性”；

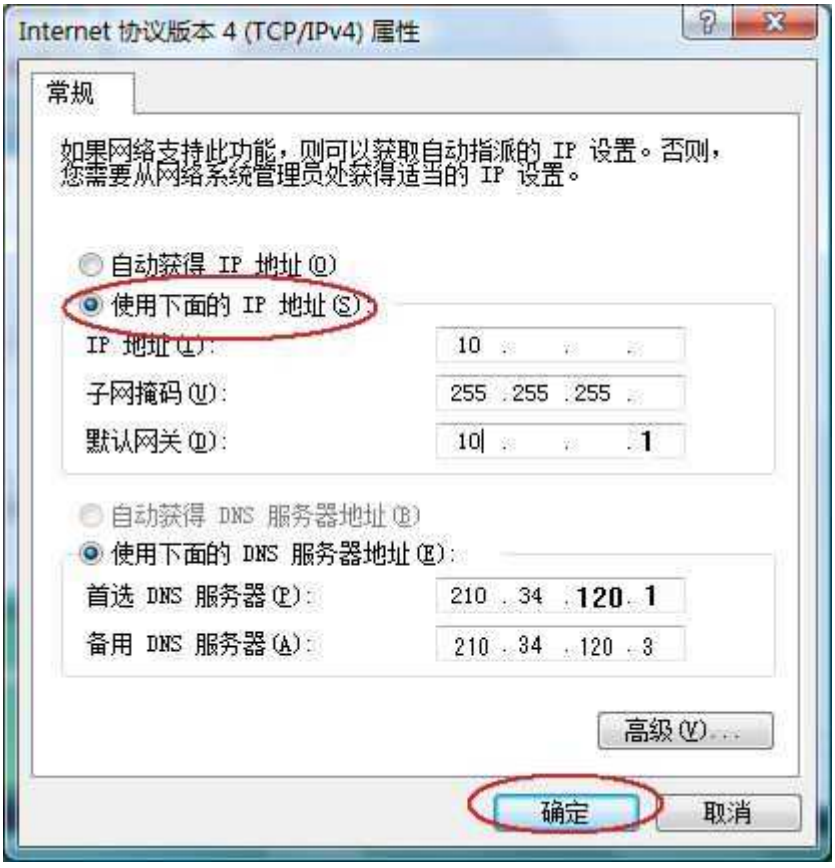
第二步：在弹出窗口处点击“管理网络连接”

第三步：双击“本地连接”，显示属性。

第四步：点击 IPV4 的属性，



第五步：选择“使用下面的 IP 地址”，输入用户 IP。



第六步：点击“确定”完成设置。

5.3 锐捷客户端及安装说明

进入 http://ipgate.qztc.edu.cn/ 页面，点击公告栏里的“客户端下载”链接下载 802.1x 登陆软件，复制到本机里安装。配置好 IP 资源，在登陆软件里正确填入统一身份认证帐号密码，经 802.1x 验证后即可接入校园网。

注：住学生宿舍的老师申请方法同学生，统一身份认证帐号为工号。

5.4 常见问题解答

在您日常的网络和计算机使用过程中，可能会遇到这样或那样的一些小问题，在这里我们在这列出一些常见故障问题，包括各位校园网用户经常提出的疑

问，希望这些可以为您解决问题提供帮助，如果在这里找不到您需要的内容，请和中心联系，我们会尽快解答。

问：网络不通、连接不了因特网怎么办？

答：当你发现网络不通时，可以按照下列步骤进行自查：

① 检查物理上的原因：网线是否脱落或松动；网卡上绿灯有没有亮。

② 若网线无脱落和不松动，且网卡上的绿灯是亮的，则使用 Ping 命令检查网络是否正常。在“开始”菜单中的“运行”里输入“cmd”,然后在命令提示符里用输入格式“ping 网关 IP 地址”进行测试（例如：ping 10.10.1.1），如果返回一系列正常消息说明本机的网卡工作正常，如果返回“Request timed out”，则表明可能网卡安装或配置有问题，也可能是你的网卡驱动有问题或 IP 设置有错误，这时需重新安装网卡驱动程序。(注意：不能自行更改 IP 设置，若自行更改也会导致网络不通，应按照分配 IP 地址时的设置)。

问：为什么访问一些网站时网速很慢？

答：造成网络速度慢的可能原因有：

①网络访问是一个端到端的访问过程，需要整个过程中的每个环节都高效运行才能保证网络访问的稳定。若外网的任何一段传输有问题，都会造成网站无法访问或速度缓慢等诸多问题。中心只能管理校园网内部的设备和线路，对于校园网以外的部分我们只能协调和测试，却不能保证能够解释和解决无法访问和访问速度的问题。如果访问其他网站正常的情况下，一般问题都处在您自己的电脑或是远端网站的服务器。

②您所访问网站的服务器响应能力。网站服务能力的好坏影响着你的访问速度，并不是所有网站的服务能力都好，有些网站访问者稍多时网站的反应速度就很慢。

③上网高峰期上网的速度会较慢，并且如果您所访问的网站刚好很多人正在访问时那么上网的速度也会较慢。

④您所使用的计算机有否有故障和性能。如被黑客攻击、感染了计算机病毒、网卡或线路有故障、打开的程序或窗口太多、计算机本身的速度很慢等，都会使您感觉到上网很慢。

问：电脑本地连接状态上打着红色小叉,连接不了网络,这是为什么?

答：这表明网络没有正确连接，须检查网络的连接情况。网卡灯是网络和电脑网卡连接的标志。网卡灯不亮证明网络和网卡之间连接有问题，需要检查网线和网卡之间是否松脱或错接，或者网卡损坏。可尝试插拔几次或更换网线。如果网卡损坏，请及时更换。如果网卡的灯显示是正常的，表明网络连接状态正常。

问：更多问题....

答：联系我们 nic@qztc.edu.cn, http://nic.qztc.edu.cn/bbs/，电话：22911950(1950)转 0，22258558（8558）转 0。

(责任编辑:cable)

第六章 政策法规

6.1 计算机信息网络国际联网安全保护管理办法

中华人民共和国公安部令（第 33 号）

《计算机信息网络国际联网安全保护管理办法》，已于 1997 年 12 月 11 日经国务院批准，现予发布，自 1997 年 12 月 30 日起施行。一九九七年十二月十六日计算机信息网络国际联网安全保护管理办法。（1997 年 12 月 11 日国务院批准，1997 年 12 月 30 日公安部发布）

第一章总则

第一条　为了加强对计算机信息网络国际联网的安全保护，维护公共秩序和社会稳定，根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和其它法律、行政法规的规定，制定本办法。

第二条　中华人民共和国境内的计算机信息网络国际联网安全保护管理，适用本办法。

第三条　公安部计算机管理监察机构负责计算机信息网络国际联网的安全保护管理工作。公安机关计算机管理监察机构应当保护计算机信息网络国际联网的公共安全，维护从事国际联网业务的单位和个人的合法权益和公众利益。

第四条　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯罪活动。

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反宪法和法律、行政法规的。

第六条 任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

第二章安全保护责任

第八条　从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

第九条　国际出入口信道提供单位、互联单位的主管部门或者主管单位，应当依照法律和国家有关规定负责国际出入口信道、所属互联网络的安全保护管理工作。

第十条　互联单位、接入单位及使用计算机信息网络国际联网的法人和其他组织应当履行下列安全保护职责：

（一）负责本网络的安全保护管理工作，建立健全安全保护管理制度；

（二）落实安全保护技术措施，保障本网络的运行安全和信息安全；

（三）负责对本网络用户的安全教育和培训；

（四）对委托发布信息的单位和个人进行登记，并对所提供的信息内容按照本办法第五条进行审核；

（五）建立计算机信息网络电子公告系统的用户登记和信息管理制度；

（六）发现有本办法第四条、第五条、第六条、第七条所列情形之一的，应当保留有关原始记录，并在二十四小时内向当地公安机关报告。

（七）按照国家有关规定，删除本网络中含有本办法第五条内容的地址、目录或者关闭服务器。

第十一条　用户在接人单位办理入网手续时，应当填写用户备案表。备案表由公安部监制。

第十二条　互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织（包括跨省、自治区、直辖市联网的单位和所属的分支机构），应当自网络正式联通之日起三十日内，到所在地的省、自治区、直辖市人民政府公安机关指定的受理机关办理备案手续。

前款所列单位应当负责将接入本网络的接入单位和用户情况报当地公安机关备案），并及时报告本网络中接入单位和用户的变更情况。

第十三条　使用公用帐号的注册者应当加强对公用帐号的管理，建立帐号使用登记制度。用户帐号不得转借、转让。

第十四条　涉及国家事务、经济建设、国防建设、尖端科学技术等重要领域的单位办理备案手续时，应当出具其行政主管部门的审批证明。

前款所列单位的计算机信息网络与国际联网，应当来取相应的安全保护措施。

第三章安全监督

第十五条　省、自治区、直辖市公安厅（局），地（市）、县（市）公安局，应当有相应机构负责国际联网的安全保护管理工作。

第十六条　公安机关计算机管理监察机构应当掌握互联单位、接入单位和用户的各案情况，建立备案档案，进行备案统计、并按照国家有关规定逐级上报。

第十七条　公安机关计算机管埋监察机构应当督促互联单位、接入单位及有关用户建立健全安全保护管理制度。监督、检查网络安全保护管理以及技术措施的落实猜况。

公安机关计算机管理监察机构在组织安全检查时，有关单位应当派入参加。公安机关计算机管理监察机构对安全检查发现的问题，应当提出改进意见，作出详细记录，存档备查。

第十八条　公安机关计算机管理监察机构发现含有本办法第五条所列内容的地址、目录或者服务器时，应当通知有关单位关闭或者删除。

第十九条　公安机关计算机管理监察机构应当负责追踪和查处通过计算机信息网络的违法行为和针对计算机信息网络的犯罪案件，对违反本办法第四条、第七条规定的违法犯罪行为，应当按照国家有关规定移送有关部门或者司法机关处理。

第四章法律责任

第二十条　违反法律，行政法规，有本办法第五条、第六条所列行为之一的，由公安机关给予警告，有违法所得的；没收违法所得，对个人可以并处五千元以下的罚款，对单位可以并处一万五千元以下的罚款；情节严重的，并可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格；构成违反治安管理行为的，依照治安管理处罚条例的规定处罚；构成犯罪的，依法追究刑事责任。

第二十一条　有下列行为之一的，由公安机关责令限期改正，给予警告；有违法所得的，没收违法所得；在规定的限期内未改正的，对单位的主管负责人员和其他直接责任人员和其他可以并处一万五千元以下的罚款，情节严重的，并可以给予六个月以内的停止联网。停机整领的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格。

（一）未建立安全保护管理制度的；

（二）未采取安全技术保护措施的；

（三）未对网络用户进行安全教育和培训的；

（四）未提供安全保护管理所需信息、资料及数据文件，或者所提供内容不真实的；

（五）对委托其发布的信息内容未进行审核或者对委托单位和个人未进行登记的；

（六）未建立电子公告系统的用户登记和信息管理制度的；

（七）未按照国家有关规定，删除网络地址、目录或者关闭服务器的。

（八）未建立公用帐号使用登记制度的；

（九）转借、转让用户帐号的。

第二十二条　违反本办法第四条、第七条规定的，依照有关法律、法规予以处罚。

第二十三条　违反本办法第十一条、第十二条规定，不履行备案职责的由公安机关给予警告或者停机整顿不超过六个月的处罚。

第五章附则

第二十四条　与香港特别行政区和台湾、澳门地区联网的计算机信息网络的安全保护管理，参照本办法执行。

第二十五条　本办法自发布之日起施行。

6.2 互联网电子公告服务管理规定

（中华人民共和国信息产业部第三号令）

第一条 为了加强对互联网电子公告服务(以下简称电子公告服务)的管理，规范电子公告信息发布行为，维护国家安全和社会稳定，保障公民、法人和其他组织的合法权益，根据《互联网信息服务管理办法》的规定，制定本规定。

第二条 在中华人民共和国境内开展电子公告服务和利用电子公告发布信息，适用本规定。

本规定所称电子公告服务，是指在互联网上以电子布告牌、电子白板、电子论坛、网络聊天室、留言板等交互形式为上网用户提供信息发布条件的行为。

第三条 电子公告服务提供者开展服务活动，应当遵守法律、法规，加强行业自律，接受信息产业部及省、自治区、直辖市电信管理机构和其他有关主管部门依法实施的监督检查。

第四条 上网用户使用电子公告服务系统，应当遵守法律、法规，并对所发布的信息负责。

第五条 从事互联网信息服务，拟开展电子公告服务的，应当在向省、自治区、直辖市电信管理机构或者信息产业部申请经营性互联网信息服务许可或者办理非经营性互联网信息服务备案时，提出专项申请或者专项备案。

省、自治区、直辖市电信管理机构或者信息产业部经审查符合条件的，应当在规定时间内连同互联网信息服务一并予以批准或者备案，并在经营许可证或备案文件中专项注明；不符合条件的，不予批准或者不予备案，书面通知申请人并说明理由。

第六条 开展电子公告服务，除应当符合《互联网信息服务管理办法》规定的条件外，还应当具备下列条件：

(一)有确定的电子公告服务类别和栏目；

(二)有完善的电子公告服务规则；

(三)有电子公告服务安全保障措施，包括上网用户登记程序、上网用户信息安全管理制度、技术保障设施；

(四)有相应的专业管理人员和技术人员，能够对电子公告服务实施有效管理。

第七条 已取得经营许可或者已履行备案手续的互联网信息服务提供者，拟开展电子公告服务的，应当向原许可或者备案机关提出专项申请或者专项备案。

省、自治区、直辖市电信管理机构或者信息产业部，应当自收到专项申请或者专项备案材料之日起60日内进行审查完毕。经审查符合条件的，予以批准或者备案，并在经营许可证或备案文件中专项注明；不符合条件的，不予批准或者不予备案，书面通知申请人并说明理由。

第八条 未经专项批准或者专项备案手续，任何单位或者个人不得擅自开展电子公告服务。

第九条 任何人不得在电子公告服务系统中发布含有下列内容之一的信息：

(一)反对宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)煽动民族仇恨、民族歧视，破坏民族团结的；

(五)破坏国家宗教政策，宣扬邪教和封建迷信的；

(六)散布谣言，扰乱社会秩序，破坏社会稳定的；

(七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(八)侮辱或者诽谤他人，侵害他人合法权益的；

(九)含有法律、行政法规禁止的其他内容的。

第十条 电子公告服务提供者应当在电子公告服务系统的显著位置刊载经营许可证编号或者备案编号、电子公告服务规则，并提示上网用户发布信息需要承担的法律责任。

第十一条 电子公告服务提供者应当按照经批准或者备案的类别和栏目提供服务，不得超出类别或者另设栏目提供服务。

第十二条 电子公告服务提供者应当对上网用户的个人信息保密，未经上网用户同意不得向他人泄露，但法律另有规定的除外。

第十三条 电子公告服务提供者发现其电子公告服务系统中出现明显属于本办法第九条所列的信息内容之一的，应当立即删除，保存有关记录，并向国家有关机关报告。

第十四条 电子公告服务提供者应当记录在电子公告服务系统中发布的信息内容及其发布时间、互联网地址或者域名。记录备份应当保存60日，并在国家有关机关依法查询时，予以提供。

第十五条 互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息，记录备份应当保存 60 日，并在国家有关机关依法查询时，予以提供。

第十六条 违反本规定第八条、第十一条的规定，擅自开展电子公告服务或者超出经批准或者备案的类别、栏目提供电子公告服务的，依据《互联网信息服务管理办法》第十九条的规定处罚。

第十七条 在电子公告服务系统中发布本规定第九条规定的信息内容之一的，依据《互联网信息服务管理办法》第二十条的规定处罚。

第十八条 违反本规定第十条的规定，未刊载经营许可证编号或者备案编号、未刊载电子公告服务规则或者未向上网用户作发布信息需要承担法律责任提示的，依据《互联网信息服务管理办法》第二十二条的规定处罚。

第十九条 违反本规定第十二条的规定，未经上网用户同意，向他人非法泄露上网用户个人信息的，由省、自治区、直辖市电信管理机构责令改正；给上网用户造成损害或者损失的，依法承担法律责任。

第二十条 未履行本规定第十三条、第十四条、第十五条规定的义务的，依据《互联网信息服务管理办法》第二十一条、第二十三条的规定处罚。

第二十一条 在本规定施行以前已开展电子公告服务的，应当自本规定施行之日起 60 日内，按照本规定办理专项申请或者专项备案手续。

第二十二条 本规定自发布之日起施行。

6.3 计算机病毒防治管理办法

第一条 为了加强对计算机病毒的预防和治理，保护计算机信息系统安全，保障计算机的应用与发展”，根据《中华人民共和国计算机信息系统安全保护条例》的规定，制定本办法。

第二条 本办法所称的计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

第三条 中华人民共和国境内的计算机信息系统以及未联网计算机的计算机病毒防治管理工作，适用本办法。

第四条 公安部公共信息网络安会监察部门主管会国的计算机病毒防治管理工作地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

第五条 任何单位和个人不得制作计算机病毒。 第六条 任何单位和个人不得有下列传播计算机病的行为：

（一）故意输入计算机病毒，危害计算机信息系统安；

（二）向他人提供含有计算机病毒的文件、软件、媒体；

（三）销售、出租、附赠含有计算机病毒的媒体；

（四）其他传播计算机病毒的行为。

第七条 任何单位和个人不得向社会发布虚假的计算机病毒疫情。 第八条 从事计算机病毒防治产品生产的单位，应当及时向公安部公共信息网络安会监察部门批准的计算机病毒防治产品检测机构提交病毒样本。

第九条 计算机病毒防治产品检测机构应当对提交的病毒样本及时进行分析、确认，并将确认结果上报公安部公共信息网络安全监察部门。

第十条 对计算机病毒的认定工作，由公安部公共信息网络安会监察部门批准的机构承担。

第十一条 计算机信息系统的使用单位在计算机病毒防治工作中应当履行下列职责：

（一）建立本单位的计算机病毒防治管理制度；

（二）采取计算机病毒安会技术防治措施；

（三）对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训；

（四）及时检测、清除计算机信息系统中的计算机病毒，并备有检测、清除的记录.

（五）使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品；

（六）对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

第十二条 任何单位和个人在从计算机信息网络上下裁程序、数据或者购置、维修借入计算机设备时，应当进行计算机病毒检测。

第十三条 任何单位和个人销售、附赠的计算机病毒防治产品，应当具有计算机信息系统安会专用产品销售许可证，并贴有“销售许可”标记。

第十四条 从事计算机设备或者媒体生产、销售、出租、维修行业的单位和个人，应当对计算机设备或者媒体进行计算机病毒检测、清除工作，并备有检测、清除的记录。

第十五条 任何单位和个人应当接受公安机关对计算机病毒防治工作的监督、检查和指导。 第十六条 在非经营活动中有违反本办法第五条、第六条第二、三、四项规定行为之一的，由公安机关处以一千元以下罚款。 在经营活动中有违反本办法第五条第六条第二、三、四项规定行为之一，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万兀。 违反本办法第六条第一项规定的，依照《中华人民共和国计算机信息系统安全保护条例》第二十三条的规定处罚。

第十七条 违反本办法第七条、第八条规定行为之一的，由公安机关对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款；对个人处以五百元以下罚款。 第十八条 违反本办法第九条规定的，由公安机关处以警告，并责令其限期改正；逾期不改正的，取消其计算机病毒防治产品检测机构的检测资格。

第十九条 计算机信息系统的使用单位有下列行为之一的，由公安机关处以警告，并根据情况责令其限期改正；逾期不改正的，对单位处以一千元以下罚款，对单位直接负责的主管人员和直接责任人员处以五百元以下罚款：

（一）未建立本单位计算机病毒防治管理制度的；

（二）未采取计算机病毒安全技术防治措施的；

（三）未对本单位计算机信息系统使用人员进行计算机病毒防治教育和培训的

（四）未及时检测、清除计算机信息系统中的计算机病毒，对计算机信息系统造成危害的；

（五）未使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品对计算机信息系统造成危害的。

第二十条 违反本办法第十四条规定，没有违法所得的，由公安机关对单位处以一万元以下罚款，对个人处以五千元以下罚款；有违法所得的，处以违法所得三倍以下罚款，但是最高不得超过三万元。

第二十一条 本办法所称计算机病毒疫情，是指某种计算机病毒爆发，流行的时间范围、破坏特点、破坏后果等情况的报告或者预报。 本办法所称媒体，是指计算机软盘、硬盘、磁带、光盘等。

第二十二条 本办法自发布之日起施行。

6.4 中华人民共和国刑法(选摘)

（1997 年 3 月 14 日第八届全国人民代表大会第五次会议通过）

第二百八十五条违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二百八十六条违反国家规定，对计算机信息系统功能进行删除、修改、增加干扰造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役后果特别严重的，处五年以上有期刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

注：以上文件摘自网络，以原文为准，供参考。

(V070301 责任编辑:wdl)

第七章 校园网相关规定

7.1 泉州师范学院校园计算机网信息发布安全管理办法

泉师院综[2003]38 号　　2003.5.15

为贯彻《中华人民共和国计算机信息系统安全保护条例》、《高等学校计算机网络电子公告服务管理规定》、《关于进一步落实我省高校校园网络安全保护工作的通知》等有关规定，切实加强校园网的安全管理工作，高度重视网络、信息安全问题，提高保密意识，加强网络安全防范，保证我校计算机网络系统的安全运行，防止泄密和传输非法信息、不健康信息，充分发挥校园网的效益，特制订本办法。

第一条 泉州师范学院校园网是中国教育科研网的一个组成部分,是我校教学、科研工作的基础设施之一。校园网严格按照国家教育部、福建省教育厅和公安部门的有关规定进行管理,在业务上接受中国教育科研网网络信息中心的指导，原则上只供学校的师生进行管理、教学和科研使用，不提供商业性服务。

第二条 校园网分为内部网和互联网两部分。除网络信息中心的地址外，不开放直接对外访问的 IP 地址，并取消各单位的各类二级代理服务器；一般用户不能提供 Internet 服务，需要 Internet 服务的用户应提出申请，要报送学校网络安全领导小组、数字校园领导小组、宣传部等有关部门的审批，获准后由网络信息中心分配 IP 地址并提供相应设置办法。

第三条 接入单位应设立网络安全员(可由信息网络管理员兼)，报校网络安全领导小组批准，并在网络信息中心登记备案。网络安全员负责本部门网络的安全保护工作，制定安全防范责任制。单位领导要加强对网络应用人员的遵纪守法教育和信息安全教育，提高安全防范意识，使操作人员具有良好的工作作风和职业道德。各单位设专人负责审查上网信息。所有用户有义务向信息网络管理员、网络信息中心和有关部门报告本部门和其它部门违法犯罪行为和有害信息，并配合有关部门查处网络违纪行为，网络管理人员保存有关记录后删除。网络用户应经常更新和妥善保管防杀病毒软件，确保防杀病毒软件本身无毒。

第四条 向学生开放的教学实验室应采取可靠措施，保证上网用户信息记录的完整准确，并采取必要的技术措施，从根源上避免病毒和黑客软件的传播。学

生上网须凭学生证等其他有效证件在指定计算机上进行浏览，并认真如实登记。不得让外来人员及非本校学生使用计算机。

第五条 网络信息中心负责校园网的日常运行与管理，同时负责学校网站的整体规划与设计、网络安全策略制订、实施以及一些公共信息的开发与应用（学校主页、OA 等），为各单位提供一个良好的技术支持平台，保障和推动我校网上信息的建设与发展。各单位应以网络信息中心创造的网络平台为依托，努力开发各类实用信息管理系统。

第六条 校园网提供公开服务的 Web 站点、域名服务器、邮件服务器等均在中国教育科研网网络信息中心进行了注册，网络信息中心配有专用设备，指定专人负责安全监控和网络技术管理，提供公共信息服务，各职能部门的信息网络管理员负责信息采集与发布，一般应用人员只有浏览权。

第七条 原则上申请主页上网的申报资格应是处级单位及相应级别的研究所。默认情况下各单位主页只对校内公开，需单独建立网站进行对外宣传的单位及个人，必须到网络信息中心申请主机托管或虚拟主机空间，并要报送学校网络安全领导小组、数字校园领导小组、宣传部等有关部门的审批。信息正式发布前须经本单位负责人(或由本单位指定网络安全负责人)签字以示负责，对校外发布还需要宣传部的审批。发布人必须对其发布的内容的真实性、安全性、保密性等负全责。

第八条 各单位开设实验性的交互式栏目（如：BBS、聊天室、留言簿、电子邮件等）,只限在校园网范围内运行，一律不准对外公开宣传，也不得在校园网外提供镜像站或链接；建立前，必须经网络安全领导小组批准后方可在校园网范围内提供服务；不经申报，擅自开放或者到校外做镜象站点的，将封闭其 IP 地址，并作严肃处理。除网络信息中心外，任何单位和个人不准提供个人主页服务。

第九条 各单位负责人是本单位网络信息安全第一责任人，负责审批本单位上网信息和交互式栏目的信息安全监控。要指定专人对本单位主页进行定期更新维护，保证所提供信息的准确、及时、全面。学校将定期对信息网络管理员、网络安全员、单位主页建设和信息维护情况进行评比检查和表彰。对上网信息审查不严,造成严重后果的，将视情节轻重追究第一责任人的连带责任。

第十条 学校公共信息统一系统采用 Brows/Server 结构，数据由各管理单位进行定期备份，对备份数据由专人进行妥善保管，确保发生意外情况时能及时恢复运行。校园网信息系统、信息来源及处理方式经校数字校园领导小组审定；软件开发由数字校园工程技术专家组进行指导。系统软件应对访问权限严格限制，对不同的操作人员、不同的信息等级分设口令。系统软件要能有监控功能，将使用过程中的重要信息记录到审计文件中，便于掌握全面情况，发现可疑现象，及时追查安全事故责任。系统管理员口令应绝对保密，根据用户需求严格控制，合理分配用户权限；管理员或系统用户口令(包括“计费网关”、代理服务器、电子邮件等网上一系列应用系统)要保密，如因泄密而引发安全事故，由帐号和口令管理者负责。

第十一条 有下列行为之一者，情节轻微者，网络信息中心可提出警告或停止其使用网络，同时报告校监察室进行查处；情节严重者，提交司法机关处理。

(一)制作、复制、发布、传播下列信息:

1.违反宪法所确定的基本原则的；

2.危害国家安全，泄露国家秘密，有颠覆国家政权，破坏国家统一言论的；

3.损害国家荣誉和利益的；

4.煽动民族仇恨、民族歧视，破坏民族团结的；

5.破坏国家宗教政策，宣扬邪教和封建迷信的；

6.散布谣言，扰乱社会秩序，破坏社会稳定的；

7.散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

8.侮辱或者诽谤他人，侵害他人合法权益的；

9.含有法律、行政法规禁止的其他内容的。

(二)破坏、盗用计算机网络中的信息资源，危害网络安全活动；

(三)对网络及联网计算机进行网络地址扫描或端口扫描，干扰网络正常运行；

(四)盗用他人帐号；

(五)不按国家和学校有关规定擅自接纳网络用户，私自转借、转让用户帐号造成危害；

(六)故意制作、传播计算机病毒等破坏性程序。

附则： 单位及个人在学校以外网站发布的任何信息，不在本办法管理之内，应有受理发布的相应组织进行管理。网络信息中心不对其安全及管理问题承担任何责任。

本办法自发布之日起执行。

附：泉州师范学院中英文网站专门信息维护分工

二〇〇三年五月十五日

7.2 泉州师范学院校园网二级管理规定

泉师院综[2003]39 号　2003.5.15

校园网将有多个核心节点和众多的分支节点，管理和维护工作量巨大。为了更好地提高网络管理效率，及时发现和排除校园网络故障，保证校园网稳定、安全、快速运营，必须实施有效的管理制度。本规定旨在规范各级网络管理及网络管理员的分工与职责。

一、二级管理职责的划分

1、校园网的管理实施二级管理制度：即网络信息中心负责学校主干网络（包括核心节点和到各建筑的线路）的管理；各接入单位负责各分支节点以及单位子网（包括校园网接入点和建筑物内部的线路）的管理。

2、网络信息中心负责校园网核心节点的设备运营，从核心节点到各个分支节点之间光纤畅通和主要网络设备的正常运行，以及各分支节点 IP 地址段的分配等。

3、各接入单位内部的设备的正常运行，内部节点的网络结构设计和实施，内部 IP 地址详细分配、主机的互连、子网的畅通均由各接入单位自行负责，网络信息中心可提供技术支持。

4、根据校园网建设的规划，校园网建设的经费用于校园网核心节点的建设和各个分支节点的上行设备及一次性设备支持。

5、分放在各个分支节点上行设备的设置、添置、升级和更新由网络信息中心统筹规划。各接入单位未经同意不得擅自挪用设备，更不准任意更换设备的设

置，如因上述原因造成的重大事故将由各个分支节点自行负责。如各接入单位需要对网络上行设备自行升级或更新应先到网络信息中心备案，同时网络信息中心将及时提供技术支持，但分支节点升级和更新的设备不得影响整个校园网网络和其它节点网络的正常运行。

6、分放在各个分支节点上行设备由各接入单位负责保管及日常维护，所有权及使用权归网络信息中心，如硬件设备发生故障，由网络信息中心负责维护。

7、网络信息中心负责全校性的信息系统的建设和电子邮件等全校性信息服务的提供与管理，各接入单位负责本单位信息系统的建立与维护和本单位的信息服务的提供与管理。

8、各接入单位必须指定一名单位领导负责本单位网络的行政管理，并指定专人作为信息网络管理员（可以兼职）负责信息网络技术工作和信息网络安全等工作。信息网络管理员由分支节点所在单位指派，并报校网络信息中心登记备案。

9、校内教工宿舍每个接入点必须指定一个信息网络管理员，由管理员负责本接入点的相关工作。

10、多个单位因地处同一个楼等因素而共同作为一个内部节点并共享网络设施时，按照设备安放位置归属。

11、网络信息中心为各个节点提供技术咨询、培训，协助各接入单位做好各子网的建立和维护工作。

二、信息网络管理员基本职责

1、统筹本单位建设和管理信息系统的建设及相应规章制度的建立。

2、负责组织对本单位网络设备、计算机系统硬、软件的维护和管理(包括放在本单位的校园网公用设备的管理)。

3、负责本单位入网计算机 IP 地址的申请、发配、登记和管理以及通讯费用的收缴等工作。

4、杜绝利用网络从事与教学、科研、管理无关的活动。进行相关的各类宣传和管理，在管辖范围内严禁利用校园网传播带有反动、淫秽内容的信息，或将校园网作为违法犯罪的工具。任何人如发现上述情况必须立刻向校有关部门报告。

5、负责本单位网络的保密管理。应加强安全意识宣传，对必须保密的信息

应严格按照有关规定执行。各单位有特殊要求应及时向校园网管理中心提出，否则发生泄密等事故，将由各接入单位承担责任。

6、负责本单位网络的安全管理。应定期检查计算机（尤其应该注意节点内部的公用机房），清理病毒及黑客程序，以保障校园网各应用系统的信息安全。

7、负责本单位管理信息系统的维护、管理、数据的后备与恢复。

8、保障校园网的正常运转。在管辖范围内严禁使用 Proxy Hunter 之类影响校园网的正常运转的各种黑客软件。一经发现，网络信息中心有权立即中断该分支节点与校园网之间的连接。

9、对具有交互功能的网页内容做好管理工作，认真整理来自各方面的建议，及时反映给有关人员并做好反馈，避免不良信息在网络上传播；如发现异常，管理员应立即向学校总值班室、网络信息中心有关负责人汇报，并及时采取关闭相关服务等必要的处理措施。

10、帮助本单位用户解决使用网络的疑难问题。组织协调本单位行政人员学会并用好管理信息系统，特别要做好基础数据的录入与更新工作，保证其准确和及时。

11、校机关各部办处的信息网络管理员还应帮助对口的行政管理人员(如教务处信息网络管理员应负责对口各系、所、中心的教务员，教学秘书及主管教务的负责人)用好管理信息系统，督促和检查对口单位的基础数据是否准确和及时。

12、负责为本部门的领导组织和提供所需的信息。

13、负责校内外的信息传输和交流。

14、负责为本单位服务的网络软件的开发，负责对本部门管理信息子系统的不断完善和优化。

15、参加各类业务学习(包括计算机业务和行政管理工作方面的业务以及参加网络信息中心举办的各种培训)，不断提高工作水平。

三、本文件解释权在校网络信息中心。

二〇〇三年五月十五日

7.3 泉州师范学院校园网服务项目及收费标准

（内容已过时，建议删除或者重新编订）

泉师院综[2003]40 号　　2003.5.15

一、总 则

泉州师范学院校园网（简称 QZTCNET）是面向全校教学、科研和管理的计算机网络，同时也是中国教育和科研网（简称 CERNET）的一个成员。参照 CERNET 的有关精神，确定 QZTCNET 建设和运行的基本原则是"集中建设，自主运行"。制定本标准总的原则是降低费率、鼓励使用、合理分担、促进发展，其基本目标和依据是：

1、促进我校网络的应用水平和范围，促进各种网络信息资源的开发和有效使用，促进教学、科研和管理的网络化、信息化。

2、加强 QZTCNET 管理，保证 QZTCNET 的良性发展。通过包括经济杠杆在内的各种方式明晰用户及 QZTCNET 管理者的责任与义务，调节用户及 QZTCNET 管理者的行为。

3、为了明晰用户责任与义务、同时也为了方便用户通过不同的接入方式与使用不同地点的计算机上网，或者多个用户共享同一台计算机上网，采用上网设备管理与上网用户管理的双轨管理的方式。

4、根据 QZTCNET 通信运行费用的实际开销情况，并参照 CERNET 和兄弟院校的做法，结合我校的具体情况制定或调整 QZTCNET 收费标准。

5、学校承担网络建设、维护、运行所需的资金，各单位和个人承担合理的部分费用（即通信运行费用、网络设施使用费等）。

6、各入网用户应当分担部分运行费用，有义务按时足额缴纳计算机网络运行管理分担费（包括管理费、服务费、信息流量费等）。各入网用户可以自愿选择有偿的用户服务，并支付相应的服务费用（称为技术支持服务费）。

二、适用范围

校园网（QZTCNET）覆盖全校各教学及办公楼、部分教师住宅区。根据用户的上述属性，可将 QZTCNET 用户分为以下四个用户群：

1、单位用户：指学校各院、系、中心、部、处(室)、馆、所等用户。其特

征是分布在教学及办公楼，上网的计算机及附属设备属国家或集体资产，以教学、科研和管理为目的使用计算机网络。该帐号仅供本部门人员使用，由本部门承担使用费用。

2、教职工用户：指本校的教职员工用户（包括访问学者、进修教师、博士后）。其特征是在学校教师住宅区私人住宅或学校教师宿舍内使用计算机上网（仅供私人使用，不对公众开放）。

3、学生用户：指本校的各类学生用户(包括进修生、代培生)。其特征是在各单位的教学、试验、科研场所使用公用计算机上网或者在学校使用自备计算机上校园网（仅供私人使用，不对公众开放）。

4、其他用户：除以上三类用户以外的经学校批准的其他用户。

QZTCNET 在通过 "光纤到楼，双绞线到桌面" 提供本地接入方式（局域网接入方式）的同时，将实现提供无线方式。

本管理办法适用于 QZTCNET 的所有上述各类用户。

三、收费的管理与用途

1、学校委托网络信息中心(简称校网中心)全面负责校园网网络用费及服务费的管理工作。

2、收取的费用主要用于弥补下列开支：

①支付 CERNET 国际通信费用。

②支付国内主干网 CERNET 分担费

③支付其它与 CERNET 运行有关的费用。

④支付网络专线费用。

⑤支付其它线路租用费用和信息流量费用。

⑥将网络延伸至用户的计算机所需的部分费用。

⑦校内信息系统建设和维护的部分费用。

四、管理与服务内容

1、网络建设服务

① 以不低于 10M 的带宽将用户所在部门、楼宇连入 QZTCNET。

② 为使用网络的部门用户分配不低于 10M 的骨干交换机端口。

③ 安装、设置、维护部门交换机、楼宇交换机。

④ 为使用网络的教师用户、学生用户分配不低于 10M 的楼宇交换机端口。

⑤ 教师用户的计算机通过户线连接到楼宇交换机。

⑥ 为每台以本地方式入网的计算机分派一个固定 IP 地址。

2、基本网络服务

① 为每个部门或个人分配一个电子邮箱。

② 获得 Internet 接入服务。

③ 获得各种网络信息服务。

④ 获得各种 LAN 应用服务。

⑤ 单位个人主页代理服务

3、技术支持服务

随着网络用户的增加及网络的广泛应用，用户在使用中的各种问题及计算机所发生的各种故障不断增加，为了更好地为用户提供及时的服务，拟为用户提供有偿的面向用户端的技术支持服务。在用户发出服务请求并交费后 24 小时内获得上门服务。服务内容有：

① 诊断设备错误的原因。

② 为用户更新，升级或重装网络应用软件。

③ 解决由于用户要更换机器，更换系统，增添新设备所引起的配置错误，软、硬件冲突等问题。

④ 解决由于计算机病毒所引起的故障。

⑤ 解决由于机器搬动，不当操作及电源故障引起的网络应用软件问题。

⑥ 解决由于网络线路（非主干线路）所引起的故障。

客户端的软硬件问题原则上由用户负责解决。服务内容不包括硬件设备的维修、操作系统等系统软件（如 WINDOWS 等）的安装，如用户确需安装，应视工作量另行付费，用户可以自愿选择是否需要上述服务项目。

五、费用种类与标准

1、“计费网关”服务及费率

新开通“计费网关”服务，费用实行月租费加流量计费，均可申请“计费网关”账号及电子邮件。“计费网关”账号的功能和收费办法如下：

1)出校访问功能

①免收开户费。

②单位用户：月租费：20 元/月•IP（账号），赠送 50M 基本量，超出基本量的按 0.05 元/1M 收取。

③教职工用户：月租费：20 元/月•IP（账号），赠送 50M 基本量，超出基本量的按 0.05 元/1M 收取。

④学生用户：月租费：2 元/月•账号，赠送 10M 基本量，超出基本量的按 0.05 元/1M 收取。

⑤其他用户：参照教职工用户或由学校确定。

2)电子邮件(E-mail)

申请“计费网关”帐号之后，经申请手续后，免费提供电子邮件信箱(20M 字节空间)，学生用户毕业后交一定的服务费可以保留电子邮件。

3)校园网络接入功能

免费接入。泉州师范学院老师在校外上网时，可以使用代理服务器方式免费接入校园网络，免费访问校内资源（帐号另外申请）。

2、主页代理服务

校内单位或教师可以申请主页代理服务，用户的计算机不需要直接出校访问，而是通过主页代理技术，使用户主页被国内或国际网络访问。主页代理服务暂时免收费。

3、我校邀请的专家和学者，均可在学校免费使用校园网。

4、技术支持服务费

费用种类	设备入网费	技术支持服务费	其他
取费标准	每次 30 元/台	每次 50 元	按时间计

六、交费方法

1、用户月应缴费用由校网中心提供。

2、各类用户缴费办法如下：

单位用户的费用从各单位的办公经费用中由财务处直接扣除。

教师用户的费用从个人的工资卡中由财务处直接扣除(不同意的需提出申请)。

学生用户和其他用户要求先预交一定的基本费，费用从帐户中逐月扣除，账

户中无余款时，账号不能使用（工资不在学校发的用户也适用），学生用户要使用“一卡通”在校网中心指定的时间、地点交费，一律不使用现金。

对外通信费按月结算，当月通信费下月初记入用户帐户。

网络费用可以预交，以减少用户到校网中心交费的次数。

七、分担费用的执行

1、对用户各种帐户的管理是由计算机自动进行的，包括开通和停止。校网中心用户服务部以电子邮件方式通知用户费用情况，用户应留意校网中心发出的电子邮件通知，或通过网络查询费用情况，及时交费，以免耽误工作。

2、如果学生用户或其他用户的账面余额连续 180 天不足支付额定流量包月费，其用户资格将被取消，并收回相关资源的使用权，停止网络服务。

3、被取消用户资格者需重新办理入网和开户手续，要交缴纳用户开户费 10 元/次后才可能重新获得用户资格。

八、附则--账号说明

帐号申请人必须签订网络安全的协议。

1、账号具有唯一性，即同一时间每个账号只能在一台电脑上使用，一旦登陆成功，其他电脑无法再通过该账号上网。

2、单位账号分配原则：每台上网的电脑分配一个账号，同时将该电脑 IP 地址与账号绑定，即该账号只能在相对应的电脑上使用。单位账号实行责任人管理原则。

3、教职工需持身份证件及其复印件由所在部门加盖公章后，至校网中心申请账号。

4、学生账号按学生学号分配账号。学生需持本人学生证预缴纳一定的费用后方能开通账号。

5、教职工和学生账号可在校园网内任何地方使用，请妥善管理好自己的账号。建议经常修改自己的密码，一旦账号被盗用，请及时与校网中心联系，并提供相应的身份证明。账号被盗用期间造成的经济损失和其他后果，由帐号管理者自负。

6、所有账号均设置统一的初始密码：888888，账号一经开通，请登陆账号管理页面，立即更改自己的密码，未及时更换密码而造成的经济损失和其他后果，

责任自负。

7、暂停：用户若较长时间内不使用网络帐号，可预先带证件到校网中心运行部办理暂停手续，暂停期间(按整月计算)月租不计。

8、退户：用户若要结束使用网络帐号，可带证件到校网中心办理退户手续，退户时，凭年内校网中心开出的校内结算凭证，可退回帐户中的余额。

9、盗用他人帐户使用网络资源，一经发现，除赔偿被盗用户的经济损失外，将视情节处以罚款或其他处罚；对拒绝处罚的单位，校网中心有权通过有关单位强制执行。

本办法自 2003 年 6 月 1 日起实行，解释权在校网络信息中心。

二〇〇三年五月十五日

7.4 泉州师范学院校园网收费标准

一、总则

泉州师范学院校园网（简称 QZTCNET）是面向全校教学、科研和管理的计算机网络，同时也是中国教育和科研网（简称 CERNET）的一个成员。为加强校园网的管理，保证校园网的良好运行和健康发展，按照国家有关法规、中国教育和科研计算机网（CERNET）有关规定、《福建省物价局、福建省财政厅、福建省教育厅关于规范高等学校和中等职业学校收费管理工作有关问题的通知》（闽价[2005]费 435 号）以及学校有关规章制度，本着“降低费率、鼓励使用、合理分担、促进发展”的原则，特制定本收费标准。

1、为了明确用户的责任与义务，同时也为了方便用户通过不同的接入方式与使用不同地点的计算机上网，或者多个用户共享同一台计算机上网，采用上网设备管理与计费帐号管理双轨分离管理的方式。

2、本着“降低费率、鼓励使用”的原则，QZTCNET 所有的网络资源一律免费，仅当用户使用互联网资源时才产生网络费用。

3、学校承担网络建设、维护、运行所需的资金，各单位和个人分担合理的

通信运行费用、网络设施使用费等中的部分费用。

4、根据 QZTCNET 运营费用的实际情况，并参照 CERNET 和兄弟院校的做法，结合我校的具体情况制定或调整本收费标准。

5、各入网用户本着自愿选择的原则，有义务及时足额缴纳网络运行管理分担费（包括管理费、服务费、信息流量费等）。

二、收费的管理与用途

1、学校委托网络信息中心全面负责校园网网络用费及服务费的管理工作，做到收支透明，随时接受监督。

2、收取的费用主要用于弥补下列开支：

①支付国内主干网 CERNET 分担费；

②支付 CERNET 国际通信费用；

③支付其它与 CERNET 运行有关的费用；

④支付网络专线费用；

⑤支付其它线路租用费用和信息流量费用；

⑥将网络延伸至用户的计算机所需的部分费用；

⑦校内信息系统建设和维护的部分费用。

三、计费帐号的分类、申请及收费标准

计费帐号为用户使用互联网网络资源时需进行认证的帐号密码，是收费的唯一依据。根据上网用户的属性，目前计费帐号分为四类。

（一）、学生用户计费帐号

1、适用对象：本校所有的学生（包括进修生、代培生等），以学号为帐号。

2、申请方法：登录计费系统进行注册，并在一周内携带证件至网络信息中心激活。

3、收费标准：免月租费，每月提供 100M 基本流量，超出的按 5 元/1000M 收取费用；帐号欠费则自动锁定，需充值至不欠费才能解锁。

4、使用期限：学生毕业。

5、使用范围：所有 QZTCNET 上网场所。

（二）、办公用户计费帐号

1、适用对象：本校所有的教职员工（包括合同工、访问学者、进修教师、博士后等），以工号为帐号。

2、申请方法：携带证件至网络信息中心开通。

3、收费标准：免月租费，每月提供 2500M 基本流量，超出的按 5 元/1000M 收取费用；帐号欠费则自动锁定，可充值至不欠费以解锁或者等待下一个自然月自动解锁。

4、使用期限：终身使用。（合同工帐号需每年至网络信息中心重新开通）

5、使用范围：所有 QZTCNET 上网场所。

（三）、教职工用户封顶计费帐号

1、适用对象：居住于校内的使用私人计算机进行上网的本校教职员工，自行设置帐号名。

2、申请方法：填写《教职工用户 IP 网关帐号申请表》，携带证件至网络信息中心开通。

3、收费标准：月租费 10 元/月，每月提供 1500M 基本流量，超出的按 5 元/1000M 收取费用，当每月总费用达到 40 元则不再增加费用；帐号欠费则自动锁定，需充值至不欠费才能解锁。若用户在一个自然月内完全不登录计费系统，则免除该月的月租费。

4、使用期限：终身使用。

5、使用范围：该帐号将与用户所使用的 IP 进行绑定，只能在特定的地方使用。

（四）、其他用户

除以上三类用户以外的经学校批准的其他用户，计费策略特殊处理。

四、交费方法

1、所有上网费用以计费帐号为唯一依据，实行不欠费方可使用原则。

2、由网络信息中心提供校园网充值卡，并在特定的场所出售，用户需自行购买充值卡进行帐号充值。

五、计费账号使用注意事项

1、用户在使用 QZTCNET 过程中应严格遵守《中华人民共和国计算机信息系统安全保护条例》（国务院令），《中华人民共和国计算机信息网络国际网络管理暂行条例》（公安部令），《泉州师院教育和科研计算机网络管理暂行规定》及其他相关法律法规，如果有违法行为由用户承担一切法律责任。

2、账号具有唯一性，即同一时间每个账号只能在一台电脑上使用。

3、用户请妥善管理好自己的账号。建议经常修改自己的密码，一旦账号被盗用，请及时与网络信息中心联系，并提供相应的身份证明。账号被盗用期间造成的经济损失和其他后果，由帐号管理者自负。

4、毕业生的学生帐号于每年 10 月－11 月期间进行删除处理，特殊情况要继续使用的请提前至网络信息中心申请延期。

5、退费：用户可携带本人身份证原件至网络信息中心退回帐户中的余额。

6、盗用他人帐户使用网络资源的，一经发现，除赔偿被盗用户的经济损失外，将视情节处以罚款或其他处罚；对拒绝处罚的，网络信息中心有权通过有关单位强制执行；情节严重的，将送由执法机关处理。

7.5 泉州师范学院数字校园应用系统管理办法(试行)

泉师院综[2005]6 号　　2005.4.13

为了加快学校信息化建设进程，进一步规范数字校园各应用系统的使用和管理，使数字校园各应用系统更好地为师生服务，特制定《泉州师范学院数字校园应用系统管理办法（试行）》。

第一条 总 则

数字校园各应用系统是校园网上的信息服务平台，承担学校公共教学、科研、管理各类信息的收集和发布。系统启用后，校内各单位对外发布或使用的公共信息应以数字校园各应用系统发布的数据为准；各单位的应用系统都应实现与公共数据库的互连，便于数据的双向通讯和共享。

网络信息中心负责数字校园各应用系统的日常维护和技术支持，各机关职能部门负责各自业务系统的管理。

第二条 最终用户范围、权利和义务

1、我校的在编教职工和在籍研究生、本专科生都是本系统的最终用户。

2、本系统所有用户的帐号和密码由网络信息中心负责发放，采用批量发放和个别发放两种方式。系统初次运行和新生入校时由各机关职能部门管理员或实体院系信息员到网络信息中心集中领取并发放。除上述情况外，用户可凭校园卡和单位证明到网络信息中心个别领取。

3、遗失密码卡或遗忘密码的用户可凭本人有效证件（学生证、身份证或校园卡)、用户密码恢复申请表到网络信息中心办理密码恢复手续。密码恢复需交纳一定手续费。

4、最终用户的权利：

（1）通过本系统查阅与本人角色相关的信息;

（2）通过本系统发布与本人有关的信息。

5、最终用户的义务：

（1）不私自将帐号和密码告知他人；

（2）发布系统要求发布的个人基本信息；

（3）对关键信息保密；

（4）不发布虚假、不真实的信息；

（5）遵守有关管理规定。

第三条 信息发布部门职责

信息发布部门指通过系统发布教学、科研、管理等方面的公文新闻、通知、公告、等信息的单位。信息发布部门的主要职责是：

1、指定一位部门主要领导分管信息化工作。

2、指定专人（部门管理员或信息员）负责本部门的信息发布任务；

3、根据各系统的要求及时收集并准确地发布信息、数据；

4、确保与各系统相连的部门服务器或其它设备在规定时间内正常运行；

5、负责审批本部门发布的信息和发布信息的人员以及保证部门网络信息安全；

6、负责校级应用系统推广使用和培训工作；

7、各单位应把应用系统的使用能力作为工作人员的基本素质要求纳入岗位

职责和能力考核范围。

第四条 超级管理员职责

超级管理员由网络信息中心指定专人担任。其主要职责是：

1、保证系统正常运行；

2、协助完成各系统主服务器的日常维护和安全管理；

3、负责各系统所有用户的初始化、帐号及密码的生成和下发；

4、负责特殊用户角色和权限的设定；

5、负责解决并记录系统运行中的异常现象；

6、与业务部门沟通，保证系统数据的完整性和真实性；

7、负责数据的备份和恢复；

8、负责过滤不良信息；

9、负责培训部门管理员和信息员；

10、负责解答用户的各类问题。

第五条 部门管理员职责

部门管理员由各部门指定专人担任。其主要职责是：

1、负责及时、准确发布本系统要求的数据和信息；

2、负责本部门发布的网上数据库的权限分配；

3、负责发布本部门的通知、公告等信息；

4、负责下发本部门所有用户的帐号和密码；

5、负责对本部门人员及相关业务人员进行使用本部门业务系统的培训；

6、参加网络信息中心组织的各类培训；

7、及时将使用中发现的问题报网络信息中心。

第六条 实体院（部）信息员职责

实体院（部）信息员由实体院指定专人担任各应用系统的使用及管理。其主要职责是：

1、负责下发本部门所有用户的帐号和密码；

2、负责向各业务系统管理员和网络信息中心报送本部门各类管理人员（教务员、科研秘书等）的名单；

3、负责发布本部门的通知、公告；

4、负责收集、整理、录入本部门各类数据。

5、负责对本部门人员进行本系统的使用指导；

6、参加网络信息中心组织的各类培训；

7、及时将使用中发现的问题报网络信息中心。

第七条 各应用系统管理办法

1、实施数字校园的各应用系统之后，除因特殊情况系统不能处理外，所有的需要处理信息数据都必须使用管理系统完成。

2、各单位在信息发生变动时,必须在第一时间内对相关系统信息进行维护，必须保证信息数据的准确性。

3、各系统管理人员必须经常对业务系统进行管理,并根据要求定期对相关信息进行统计和汇总，打印备案并加盖公章.

4、为保证信息处理的快捷性，有关人员应经常进入系统查看有无需要自己处理的事宜。

第八条 应用系统数据和文件的效力

1、常用的数据统计报表都应从相关应用管理系统打印，加盖公章后即可正式对外公布。

2、应用系统的数据应作为所有原始数据的权威数据源，各部门所涉及的数据都以应用系统数据为准。

3、各单位可以从各应用系统中以纸质形式复制公开发布的公文，注明复制单位、日期、份数并加盖复制单位的公章后，在该单位内与被复制的原始信息具有同等效力。

4、非公开发布的信息数据，各部门和个人不准复制成纸质形式作正式文件使用。

5、校内（除拟作纸质档案外）将逐步停止使用纸质形式管理基本信息数据和文件。

第九条 系统安全与保密

1、所有用户应认真贯彻执行《中华人民共和国计算机信息系统安全保护条例》和公安部《计算机信息网络国际联网安全保护管理办法》，严格遵守《中国教育和科研计算机网暂行管理办法》和学校的有关管理规定。

2、所有用户不得利用各应用系统从事危害国家、集体和他人利益的活动，不得在系统上制作、传播有碍社会治安和不健康的信息，不得制造和输入计算机病毒以及其他危害系统安全的数据。

3、所有用户应按规定的权限阅读和使用系统提供的信息。不得盗用他人用户账号，不得干扰其他用户和破坏系统服务。

4、所有用户应保管好自己的帐号，应经常更改口令并保守秘密，以防他人有意或无意打开系统数据库获取信息，滥发电子邮件、恶意增删资料或干扰系统正常运转。

5、所有使用该系统的人员均有保密的责任。不得随意发布涉及国家和学校机密以及其它不宜发布的信息。

第十条 责任与处罚

1、为了保障各应用系统的硬件、软件和信息的安全，保证系统的正常运行，所有用户应遵守本管理办法，违反者应承担相应责任。

2、对影响到业务系统正常接收、处理、传送、存档，导致系统不能正常运转的单位，学校将予以通报批评。

3、对违反本办法第九条规定，造成不良影响、导致系统损坏等后果者，给予行政处分；造成经济损失的，学校可要求其予以经济赔偿。

4、对违反本办法及国家有关法律、法规的规定，给国家、集体或他人权益造成损失者，应当依法承担相应法律责任。

第十一条 附 则

本规定由网络信息中心负责解释。

泉州师范学院

2005 年 4 月 13 日

(责任编辑:chm)

第八章 资源和服务导航

8.1 校内网络与服务资源

详见：
http://www.qztc.edu.cn/xxgk/ResourceNavigation.htm

(责任编辑:wdl)

8.2 网络服务导航和指南

详见网络信息中心工作流程。

V2.00-090928